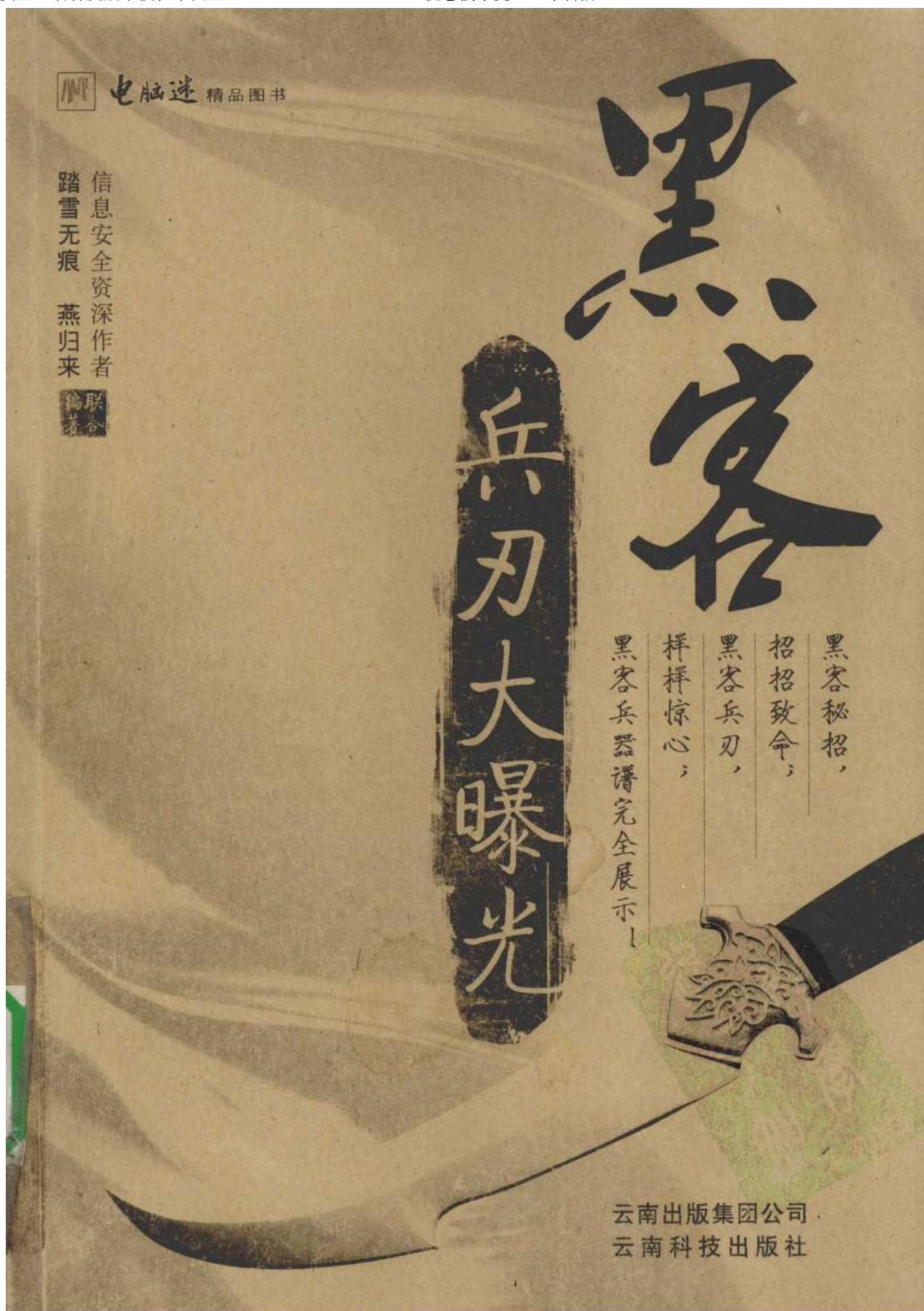


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

为什么购买

开篇声明：本书仅从技术角度出发，对黑客的各种攻击入侵工具以实例的形式进行展示，全部是经过实战检验的。但——害人之心不可有，读者请勿将本书内容用于任何违法行为，否则一切法律责任请自负！

黑客秘笈，招招致命！
黑客兵刃，样样惊心！
这就是你的黑客兵器谱！

- 黑客攻击真实案例的图解讲述，以实战讲解黑客的工具的用法
- 黑客兵器的修炼秘笈，带你进入真实世界的“黑客帝国”

本书适用于对网络安全及黑客工具应用感兴趣的读者，旨在增强网民的安全防范意识，减少电脑和网络的安全隐患。

光盘内容：

- 视频讲解黑客软件的操作过程
- 直接观看各类黑客工具的具体操作

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

光盘使用说明

特别说明：本光盘提供的黑客软件演示仅供研究使用，切勿利用来破坏他人的计算机或数据，否则一切后果自负。

点击任意视频按钮，即可直接播放界面列表中的黑客教学视频。



【光盘主界面】

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

溜客安全信息网

www.176ku.com

所提供书籍只限于技术参考时使用

请选择到官方论坛购买期刊支持正版书籍

本电子书严禁在淘宝开店出售，

禁止当做VIP收费项目等

尽量在本站下载安全的电子书刊

溜客精神：

技術共享，資源共享，資料共享

不求最好，只求較好

做中國較好的網絡安全資料站

及时访问溜客安全网

第一时间下载技术资料

请将本站推荐给更多的好友

让大家都能成为溜客一员

溜客資料共享群：

访问溜客安全网最下方
查看本站最新共享QQ群

加入溜客資料共享群超大共享FTP等你来用

請勿重複加入群，給他人一點加入的空間

目录

CONTENTS

P1

第1章 黑客常用系统命令

1.1 操作系统与MS-DOS	2
1.1.1 DOS简介及原理	2
1.1.2 Windows NT/2000/XP下的启动法	3
1.2 ping命令	6
1.2.1 使用方式图解	6
1.2.2 使用实战	6
1.3 net和nerstat命令	11
1.3.1 使用方式图解	11
1.3.2 使用实战	17
1.4 telnet和ftp命令	19
1.4.1 使用方式图解	19
1.4.2 使用实战	20
1.5 tracert命令	22
1.5.1 使用方式图解	23
1.5.2 使用实战	24
1.6 ipconfig命令	24
1.6.1 使用方式图解	24
1.6.2 使用实战	25
1.7 route命令	26

1.7.1 使用方式图解	26
1.7.2 使用实战	27
1.8 netsh命令	28
1.8.1 使用方式图解	28
1.8.2 使用实战	28
1.9 arp命令	29
1.9.1 使用方式图解	29
1.9.2 使用实战	30
1.10 小结	30

P35

第二章 IP及端口扫描工具

2.1 IP地址的查找及锁定	36
2.1.1 由网址查找IP	36
2.1.2 查找电子邮件发送者IP	37
2.1.3 查找远程局域网用户的IP	38
2.1.4 用珊瑚虫版QQ了解聊天用户IP	40
2.1.5 用IP地址定位器定位真实地理地址	41
2.2 IP扫描	42
2.2.1 使用Angry IP Scanner检测IP动态	42

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.2.2 局域网IP扫描工具	44
2.3 IP隐藏保护	45
2.3.1 用Hide IP Platinum隐藏你的真实IP	45
2.3.2 用IP地址随意换自由切换IP	46
2.3.3 干扰IP扫描工具的检测	48
2.4 端口基础知识介绍	50
2.4.1 端口的含义	50
2.4.2 TCP/IP协议	51
2.4.3 端口扫描的概念及分类	53
2.4.4 常见端口扫描技术	53
2.4.5 重要的常用端口介绍	54
2.5 小结	56

P57 第三章 聊天黑客工具

3.1 QQ盗号工具	58
3.1.1 QQ简单盗	58
3.1.2 QQ流感大盗	60
3.1.3 剑盟QQ盗号王	61
3.1.4 QQ防盗介绍及密码取回	63
3.1.5 简单反击盗QQ者	69
3.2 QQ聊天记录查看工具	70
3.2.1 QQ聊天记录器	70
3.2.2 QQ聊天终结者	73
3.2.3 DetourQQ	76
3.2.4 不用软件手工查看QQ聊天记录	78
3.2.5 QQ聊天记录保密	79
3.3 小结	82

P84 第四章 邮件黑客工具

4.1 网页邮箱暴力破解	84
4.1.1 暴力破解原理	84
4.1.2 用溯雪暴力破解邮箱密码	84
4.1.3 轻松利用163邮箱破解器登陆163邮箱	86
4.1.4 黑雨-邮箱密码破解器破解POP3邮箱	87
4.2 破解邮箱客户端软件	89
4.2.1 Foxmail软件介绍	89
4.2.2 用Foxmail杀手获得Foxmail账户密码	89
4.2.3 Foxmail账户密码保护	91
4.3 电子邮件攻击	91
4.3.1 电子邮箱信息攻击原理	91
4.3.2 随心邮箱炸弹	92
4.3.3 邮箱炸弹的防范及垃圾邮件的过滤	94
4.4 小结	102

P103 第五章 网吧及网络游戏黑客工具

5.1 网游盗号	104
5.1.1 网游账号隐患	104
5.1.2 用魔兽世界黑眼睛盗取游戏密码	104
5.1.3 用热血江湖密码幽灵获得热血江湖密码	106
5.1.4 用联众盗号机偷窥联众棋牌账号密码	107
5.1.5 网游账号安全保护	108
5.2 网游作弊	109
5.2.1 外挂作弊器简单介绍	109
5.2.2 用记牌器轻松记牌	109
5.2.3 CS作弊器及反作弊器	110

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5.2.4 魔兽世界加速外挂	112
5.3 突破网吧管理工具	113
5.3.1 跳过管理验证 Pubwin4.3修改程序	114
5.3.2 美萍9.0密码破解器	116
5.3.3 万象2R最新版破解器	117
5.3.4 网吧管理集成破解器	118
5.4 网吧密码解密工具	120
5.4.1 小哨兵密码清除器	120
5.4.2 解锁安全器2.0	120
5.4.3 BIOS密码探测器	122
5.4.4 注册表解锁器	123
5.4.5 网上邻居密码破解器	125
5.5 小结	124

P₁₂₅ 第六章 网页黑客工具

6.1 网页密码破解工具	126
6.1.1 破解原理及方法介绍	126
6.1.2 流光	126
6.1.3 AccessDiver	132
6.1.4 黑雨——网页密码破解器	138
6.2 网页漏洞扫描工具	140
6.2.1 网页漏洞简单介绍	140
6.2.2 CMXploite	146
6.2.3 N-Stealth	148
6.2.4 网页扫描和探测——IntelliTamper	151
6.3 动网论坛入侵揭密	152
6.3.1 猜测数据库路径暴力猜解管理员密码	152

6.3.2 SQL注入攻击方法	154
6.3.3 COOKIE欺骗	157
6.3.4 动网上传利用程序	161
6.4 小结	166

P₁₆₇ 第七章 文档密码破译工具

7.1 密码破译工具	168
7.1.1 显示星号密码工具	168
7.1.2 Windows操作系统登录密码破译	169
7.1.3 Office文档密码破译工具	174
7.1.4 用RAR Key 轻松打开加密RAR压缩文件	179
7.1.5 Advanced PDF Password Recovery	181
7.1.6 BIOS密码破解	182
7.1.7 破解加密光盘	186
7.2 密码破译工具防范	189
7.2.1 防范原理和手段	189
7.2.2 加密实例	190
7.3 系统EFS加密解密	201
7.3.1 EFS简单介绍	201
7.3.2 用EFS加密文件	203
7.3.3 备份加密证书	204
7.3.4 解密用EFS加密的文件	205
7.4 小结	208

P₂₀₉ 第八章 共享软件的加解密工具

8.1 软件的加密及解密基础	210
-----------------------------	------------

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8.1.1 软件的加密技术基础	210
8.1.2 软件的解密技术基础	211
8.1.3 软件加密解密流程	212
8.2 共享软件的加密	213
8.2.1 给软件加壳保护共享软件	213
8.2.2 添加反跟踪保护共享软件	214
8.2.3 增加注册认证保护共享软件	218
8.2.4 codefantasy软件加密解决方案	221
8.3 共享软件解密	223
8.3.1 反汇编解密	224
8.3.2 制作内存注册机	228
8.4 暴力破解共享软件	233
8.4.1 破解的原理及方法	233
8.4.2 爆破的条件	235
8.4.3 快速找爆破点	236
8.4.4 进行爆破	239
8.5 小结	242

P₂₄₃ 第九章 远程控制工具

9.1 木马介绍	244
9.1.1 木马的功能和分类	244
9.1.2 木马的隐藏方式	246
9.1.3 木马的启动方式	247
9.2 木马追踪防范	250
9.2.1 DLL木马追踪防范	252
9.2.2 网页木马追踪防范	255
9.2.3 反弹式木马追踪防范	258

9.3 远程控制软件介绍	259
9.3.1 冰河	259
9.3.2 广外女生	266
9.3.3 黑洞	268
9.3.4 灰鸽子	271
9.3.5 Windows自带网络远程控制	273
9.4 小结	276

P₂₇₇ 第十章 局域网黑客工具

10.1 局域网安全介绍	278
10.1.1 局域网基础知识介绍	278
10.1.2 局域网安全隐患	280
10.2 局域网密码探测工具	282
10.2.1 Share Password Checker	282
10.2.2 局域网网络密码探测器	282
10.2.3 局域网QQ号码嗅探器	290
10.3 局域网查看控制工具	291
10.3.1 LAN Explorer	292
10.3.2 NetSuper	295
10.4 局域网攻击工具	297
10.4.1 全自动局域网在线机器攻击机	298
10.4.2 局域网IP炸弹	299
10.4.3 局域网终结者	299
10.4.4 EtherPeek NX获取局域网的账号密码 ...	300
10.5 无线局域网黑客工具	303
10.5.1 无线局域网搜索工具	303
10.5.2 破解无线网络工具	308
10.6 小结	311

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

**你
想
换
吗
？**

www.17huan.com

第1章 黑客常用系统命令

在学习黑客技术之前，对计算机操作系统以及黑客常用命令有一个全面的了解是必要且非常关键的，因为使用系统命令是黑客技术的基石。本章将为读者介绍一些黑客常用的系统命令。

本章要点

- ◎ 操作系统
- ◎ DOS操作系统
- ◎ ping命令
- ◎ net和netstat命令
- ◎ telnet和ftp命令
- ◎ tracert命令
- ◎ ipconfig命令
- ◎ route命令
- ◎ netsh命令
- ◎ arp命令

1.1 操作系统与MS-DOS

操作系统是管理计算机硬件的程序，它为应用程序提供基础，并且充当计算机硬件和计算机用户的中介。所以，操作系统是用户操作计算机的基础。常见的操作系统有Windows、Linux、Unix、DOS等。

1.1.1 DOS简介及原理

DOS (Disk Operation System) 的全称是磁盘操作系统，DOS主要是一种面向磁盘的系统软件。打个比喻，DOS就是人与机器的一座桥梁，是罩在机器硬件外面的一层“外壳”，有了DOS，就不必去深入了解机器的硬件结构，也不必死记硬背那些枯燥的机器命令，只需通过一些接近于自然语言的DOS命令，就可以轻松地完成绝大多数的日常操作。另外，DOS还能有效地管理各种软硬件资源，对它们进行合理的调度，所有的软件和硬件都在DOS的监控和管理之下，有条不紊地进行着自己的工作。

DOS主要由三个基本文件和一些外部命令构成。这三个基本文件是 MSDOS.SYS，IO.SYS 和COMMAND.COM（如果是PC-DOS，则为IBMDOS.COM，IBMBIO.COM和 COMMAND.COM）。

(1) MSDOS.SYS称为DOS内核（可见MSDOS.SYS是个非常重要的文件），它主要是用来管理和启动系统的各个部件，为DOS的引导作好准备工作。

(2) IO.SYS（IO为Input&Output的缩写，意即“输入输出”）主要负责系统的基本输入和输出，即 DOS与各部件之间的联系。

(3) COMMAND.COM文件（COMMAND是“命令”的意思）是DOS与用户的接口，它主要提供了一些DOS的内部命令，接受、判别并执行用户输入的命令。磁盘是否具有启动DOS的能力，就看是否具备这三个文件，具有这三个文件的磁盘，就称作引导盘。而除此之外还包含许多 DOS外部命令的磁盘则称为系统盘，如图1-1所示的基本的DOS命令。



【图1-1】基本的DOS命令

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 1 章 黑客常用系统命令

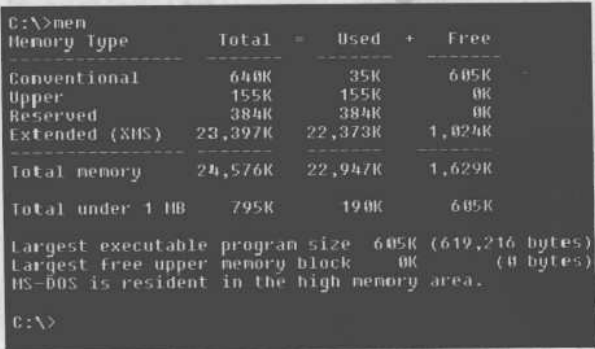
自从DOS在1981年问世以来，版本就不断更新，从最初的DOS1.0升级到了最新的DOS8.0（Windows ME系统），纯DOS 的最高版本为DOS6.22，如图1-2所示的DOS6.22版本在虚拟机上的效果。这以后的新版本DOS都是由Windows系统所提供的，并不单独存在。



【图1-2】DOS6.22版本在虚拟机上的效果

DOS的优点是快捷。熟练的用户可以通过创建BAT或CMD批处理文件完成一些烦琐的任务，通过一些判断命令（IF、|）甚至可以编写一些小程序。因此，即使在Windows XP下CMD还是高手的最爱。目前常用的DOS包括：MS-DOS（微软公司出品）、PC-DOS（IBM公司出品）、FreeDOS、ROM-DOS等，眼下流行的Windows系统是以MS-DOS为基础的。

MS-DOS的主要功能是进行内存管理、文件管理和输入/输出管理。为了实现这些功能，MS-DOS主要由四个部分组成：文件管理系统、输入/输出管理系统、命令处理系统和外部命令集，如图1-3所示。



【图1-3】MS-DOS命令行格式

1.1.2 Windows NT/2000/XP下的启动法

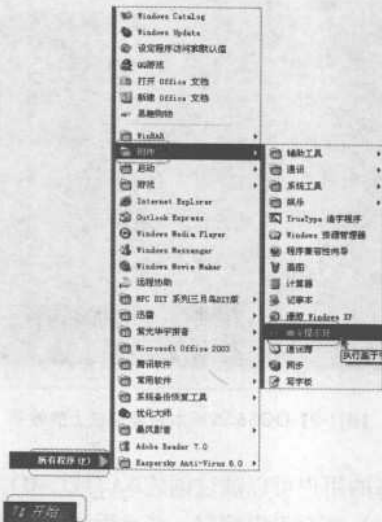
在WindowNT/2000/XP下，系统提供了一个字符操作界面，可以在此界面下运行DOS命



令，进行操作，而且不必进行Window操作系统与DOS操作系统之间的转换，比较便捷高效，本章中的DOS命令均在此字符界面进行操作，下面介绍运行“DOS的字符界面”的三种方法。

方法一：利用开始菜单进入DOS字符界面

(1) 依次单击执行“开始→程序→附件→命令提示符”命令，如图1-4所示。



【图1-4】“命令提示符”选项

(2) 弹出“命令提示符”界面，如图1-5所示。在此界面输入DOS命令，例如输入：ipconfig/all（查看IP地址）命令，然后单击回车键即可执行。



【图1-5】“命令提示符”界面

方法二：使用“搜索”功能进入DOS字符界面

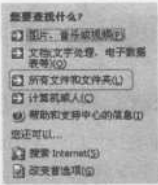
- (1) 单击“开始”按钮，在弹出的开始菜单中单击“搜索”选项，如图1-6所示。
- (2) 在搜索界面中单击“所有文件和文件夹”，如图1-7所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 1 章 黑客常用系统命令

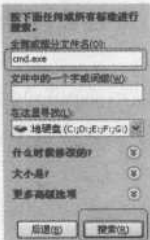


【图1-6】“搜索”选项



【图1-7】“搜索”界面

- (3) 在搜索的“全部或部分文件名”中输入“cmd.exe”，然后单击“搜索”按钮，如图1-8所示。
- (4) 开始搜索，在搜索结果中会出现一个C盘盘符标志的名为“cmd”的文件，如图1-9所示。双击该文件即可弹出用于键入DOS命令的命令提示符界面。



【图1-8】搜索内容



【图1-9】搜索结果

方法三：通过“运行”命令启动

- (1) 单击“开始”按钮，在弹出的开始菜单中单击“运行”选项，如图1-10所示。



【图1-10】“运行”选项

- (2) 在弹出的“运行”对话框中输入“cmd”命令，然后单击“确定”按钮，如图1-11所示。即可弹出用于键入DOS命令的命令提示符界面了。



【图1-11】运行命令

1.2 ping命令

Ping是用来进行网络连接测试的一个程序，对应的文件名为“Ping.exe”（在Windows XP系统下此文件存在于 C:\Windows\System32文件夹下）。此工具的最简单的用法是：“Ping xxx.xxx.xxx.xxx”（欲测试的IP地址），根据不同的测试目的可以带上不同的参数。使用 ping 可以测试计算机名和计算机的IP地址，验证与远程计算机的连接，通过将icmp回显数据包发送到计算机并侦听回显回复数据包来验证与一台或多台远程计算机的连接，此命令只有在安装了TCP/IP协议后才可以使用的。

1.2.1 使用方式图解

Ping命令的使用很简单，键入ping后，再空格，然后键入一个IP地址。那么就会显示此IP地址的响应时间等信息，以显示是否连接。

Ping命令既可以用来ping自己的IP地址检查网络状况。又可以用来ping网络中其他计算机的IP地址，比如要传文件给网络中其他计算机之前，可以用ping命令测试其他计算机是否开机或者网络是否畅通，如图1-12所示。



【图1-12】ping命令测试其他计算机

1.2.2 使用实战

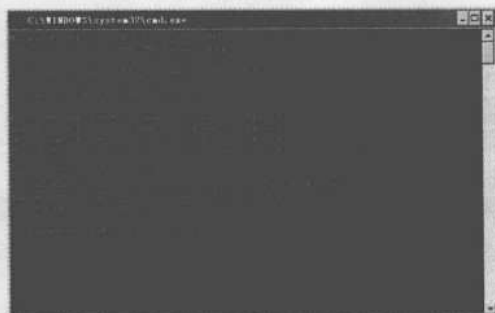
ping的一个重要用途是检查和排除本机网络故障。

巧妙使用ping命令可以快速排查网络故障。如果计算机接入互联网后，发现不能上网，则使用ping命令，逐步进行一系列测试，就能够找到并排除故障。

【案例1-1】使用ping命令排查网络故障，操作步骤如下：

1.ping 127.0.0.1

测试环回地址是否正常。如果ping命令返回正常，表明计算机安装的TCP/IP协议工作正常，如图1-13所示。



【图1-13】 ping 127.0.0.1



127.0.0.1是网卡的环回地址。所谓环回地址，是在网卡的网络接口处设置一个环回路径，用于将本机发出的目的地到本机的报文，通过环回路径送回给本机上层协议，以用来测试自身网络协议是否工作正常。环回地址也可以用来进程间通信。

2.ping 本机IP地址

本机IP地址可以通过自动分配获得，也可以人工配置。如果事先不知道本机的IP地址，可以通过ipconfig命令查看（具体内容参看1.6节）。这里设本机IP地址为127.36.78.30，如图1-14所示。



【图1-14】 ping本机IP地址

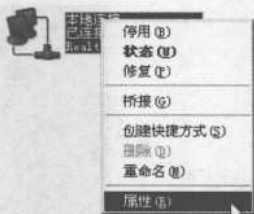
手动配置IP地址，首先需要询问网管，从网管处获得配置所需的参数。配置的方法如下：

- (1) 在桌面“网上邻居”图标上单击鼠标右键，在弹出的下拉菜单中选择“属性”命令，如图1-15所示。
- (2) 在弹出的“网络连接”窗口中，“本地连接”图标上单击鼠标右键，在弹出的菜单中单击“属性”，如图1-16所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

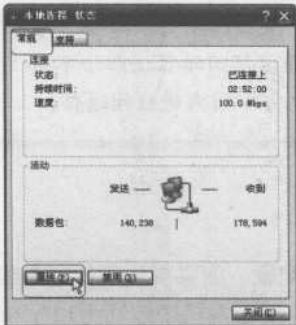


【图1-15】“网上邻居”中单击“属性”



【图1-16】“本地连接”中单击“属性”

- (3) 在弹出的“本地连接 状态”对话框中，在“常规”选项卡下，单击“属性”按钮，如图1-17所示。
- (4) 在弹出的“本地连接 属性”对话框中单击“Internet协议 (TCP/IP) 属性”，然后单击“属性”按钮，如图1-18所示。

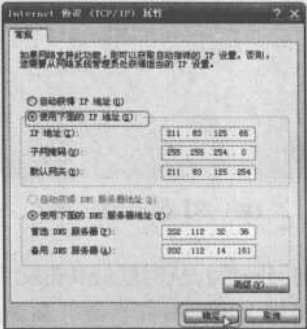


【图1-17】“本地连接 状态”对话框



【图1-18】“本地连接 属性”对话框

- (5) 在弹出的“Internet协议 (TCP/IP) 属性”对话框中配置IP地址、子网掩码、默认网关以及DNS等信息。由于是手动设置，所以先选择“使用下面的IP地址”，然后分别输入IP地址、子网掩码、默认网关和DNS服务器地址，最后单击“确定”按钮完成设置，如图1-19所示。



【图1-19】配置IP地址

- (6) 如果在自动分配中分得了IP地址，那么在“Internet协议 (TCP/IP) 属性”对话框

中就是选择的“自动获得IP地址”，不需要用户输入IP地址、子网掩码等信息，也称为动态IP地址，是基于DHCP机制的。由于DHCP的机制，IP地址有一定的租用期限，期限一到，就必须重新申请IP地址，此时IP地址可能发生变更，如果想使IP地址固定，比如在局域网中的与共享打印机相连的打印机，或者开设了FTP或者HTTP服务的计算机，也可以先用ipconfig命令查看当前分得的IP地址，然后再把查看得到的信息，根据前三个步骤的配置方法，把IP地址固定下来。

如果ping返回正常，表明网卡到外部网络物理线路连接正常。

如果出现“Destination host unreachable.”的提示，如图1-20所示，表明本地网络不能正常工作。可能是网卡工作不正常，或者网线工作不正常。其中最大的可能是网线没有插好，或者网线发生断裂等导致本机不能和网络通信。可以用测线仪等设备检查网线的通断，确定网线没有问题后，重新将网线连接到本机网卡，一般可以排除故障。



【图1-20】ping返回“Destination host unreachable.”

3.ping 局域网内网关IP地址

Ping网关的主要作用是看局域网的网关路由器是否能作出正确回答。一般网关路由器的IP地址是本网络的第一个IP，如果能够ping通，说明路由器提供服务，可以通过路由器接入到外部网络，如图1-21所示。

如果路由器没有响应，必须检查和配置网关路由器，让其为本局域网内部的机器提供接入和转发服务。

如果不知道网关路由器地址，可以通过ipconfig命令（具体内容参看1.6节）来获得。



【图1-21】ping网关IP地址

注意：IP地址和IP子网的分配是黑客的必备知识，这些知识将在第二章中讲解。

4.ping 远程服务器IP和ping远程服务器域名

ping远程服务器IP可以确定网关转发是否正常，如果ping正确返回，表明用户能够成功访问Internet。这里以新浪网一台服务器的IP地址（202.112.8.2）为例，如果正常就出现如图1-22所示的“Reply from”、“bytes”、“time”、“TTL”四个字段。

```
C:\Documents and Settings\Administrator>ping 202.112.8.2
Pinging 202.112.8.2 with 32 bytes of data:
Reply from 202.112.8.2: bytes=32 time=324ms TTL=56
Reply from 202.112.8.2: bytes=32 time=318ms TTL=56
Reply from 202.112.8.2: bytes=32 time=319ms TTL=56
Reply from 202.112.8.2: bytes=32 time=324ms TTL=56
```

【图1-22】 ping远程服务器IP

如果不能ping通，则出现如图1-23所示的“Request timed out（响应超时）”字样。

```
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32\cmd.exe>ping 202.112.8.2
Pinging 202.112.8.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

【图1-23】 “Request timed out（响应超时）”

注意：如果ping一台特定的远程服务器IP失败，可能是由于远程服务器本身的问题。可以尝试ping其他的远程机器，来确定用户是否真正能访问Internet。

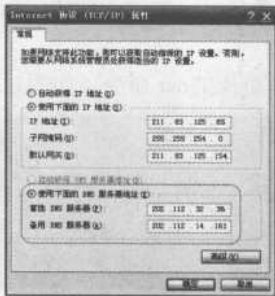
ping远程服务器IP正常以后，则尝试ping远程服务器的域名。以 www.sina.com.cn为例，如图1-24所示。

```
C:\Documents and Settings\Administrator>ping www.sina.com.cn
Pinging www.sina.com.cn [70.142.8.21] with 32 bytes of data:
Reply from 70.142.8.21: bytes=32 time=114ms TTL=56
Reply from 70.142.8.21: bytes=32 time=114ms TTL=56
Reply from 70.142.8.21: bytes=32 time=114ms TTL=56
Reply from 70.142.8.21: bytes=32 time=115ms TTL=56

Ping statistics for 70.142.8.21:
    Packets: Sent = 4, Received = 4, Loss = 0.0%, 4/4 TTL=56
    Round-trip times: Min = 114ms, Max = 115ms, Average = 114ms
```

【图1-24】 ping远程服务器名字

如果能正常通信，表明本机的DNS配置设置正确。DNS的设置可以简单通过Windows提供的TCP/IP网络配置图形界面来设置，如图1-2-15所示，设置的方法，在前面已经讲述过了，这里不再重复阐述，也可以通过netsh命令来设置。



【图1-25】Internet协议属性对话框

如果ping不成功，表明系统DNS设置错误。只需将DNS设置到可以访问的最近的DNS服务器，就可以使网络通信恢复正常。



从上面新浪网的例子中学到可以利用“ping远程服务器域名”命令来实现域名对IP地址的转换功能，“ping远程服务器域名”，ping通以后会出现相应的IP地址。

如果上面所列出的所有步骤中Ping命令都能正常返回，计算机进行本地和远程通信的功能基本正常。但是，这些命令的成功并不表示所有的网络配置都没有问题，例如，某些子网掩码错误就可能无法用这些方法检测到。

1.3 net和netstat命令

net命令是windows设置和控制IP网络的高级命令。许多Windows服务器的网络命令都以net开始。

netstat顾名思义就是一种显示网络状态的工具。它用于显示与IP、TCP、UDP和ICMP协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

通过netstat命令可以很快获取当前计算机上所有的TCP连接的状态，并查看它们使用了哪些端口。也可以查看计算机上的UDP协议占用了哪些端口。如果计算机感染了木马病毒，木马程序会打开系统后门，也就是打开某些TCP或者UDP端口和互联网上其他机器进行通信。如果熟练掌握了netstat命令的用法，就可以比较容易地监控计算机的网络通信，对一些致命木马和病毒的攻击能够提前发现，提前预防。

1.3.1 使用方式图解

net命令的使用都是在net后面跟命令的参数，键入net后，再空格，然后键入参数。net命令

1.net config

作用：显示当前运行的可配置服务，或显示并修改某项服务的设置。

格式：net config service options

参数：

- (1) 键入不带参数的net config显示可配置服务的列表。
- (2) service通过net config命令进行配置的服务（server或workstation）。
- (3) options服务的特定选项。

例：net config workstation 注释：了解本机的配置信息，如图1-29所示。



【图1-29】 net config workstation命令

2.net send

作用：向网络的其他用户、计算机或通信名发送消息。

命令格式：Net send {name | * | /domain[:name] | /users} message

有关参数说明：

- (1) name要接收发送消息的用户名、计算机名或通信名
- (2) * 将消息发送到组中所有名称
- (3) /domain[:name]将消息发送到计算机域中的所有名称
- (4) /users将消息发送到与服务器连接的所有用户
- (5) message作为消息发送的文本

例：向本机所在的域内所有主机发送一条“I have sent you a message”的消息，只需要输入命令：

```
net send * "I have sent you a message"
```

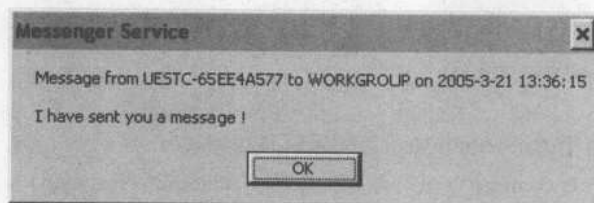
这里符号“*”表示向域内所有机器广播发送消息，如图1-30所示。



【图1-30】 net send * “I have sent you a message !”

收到这条消息的主机立即在屏幕上弹出窗口，内容为刚才键入的“I have sent you a

message”，如图1-31所示。



【图1-31】系统收到一条net send发出的网络消息

注意：

- (1) 要发送和接收消息必须首先运行信使服务。可以用net start messenger命令打开信使服务。
- (2) 从安全角度出发，建议关闭信使服务。用net stop messenger命令关闭信使服务。

3.net start /net stop

作用：net start用于启动服务，或显示已启动服务的列表。net stop用于停止系统的某个网络服务。

例：键入不带参数的 net start 显示正在运行服务的列表，如图1-32所示。



【图1-32】net start命令

4.net statistics

作用：显示本地工作站或服务服务的统计记录。

命令格式：net statistics [workstation | server]

参数介绍：

- (1) 键入不带参数的net statistics列出其统计信息可用的运行服务，如图1-33所示。
- (2) workstation显示本地工作站服务的统计信息。
- (3) server显示本地服务器服务的统计信息。



【图1-33】net statistics命令

5.net share

作用：创建、删除或显示共享资源。

命令格式：net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]

参数介绍：

- (1) 键入不带参数的net share显示本地计算机上所有共享资源的信息，如图1-34所示。
- (2) sharename是共享资源的网络名称。
- (3) drive:path指定共享目录的绝对路径。
- (4) /users:number设置可同时访问共享资源的最大用户数。
- (5) /unlimited不限制同时访问共享资源的用户数。
- (6) /remark:"text"添加关于资源的注释，注释文字用引号引住。



【图1-34】net share命令

6.net continue

作用：重新激活挂起的服务。

命令格式：net continue service

例：net continue server，如图1-35所示。



【图1-35】net continue server命令

7.net time

作用：使计算机的时钟与另一台计算机或域的时间同步。

命令格式：net time [\computername | /domain[:name]] [/set]

参数介绍：

- (1) \computername要检查或同步的服务器名。
- (2) /domain[:name]指定要与其时间同步的域。
- (3) /set使本计算机时钟与指定计算机或域的时钟同步。

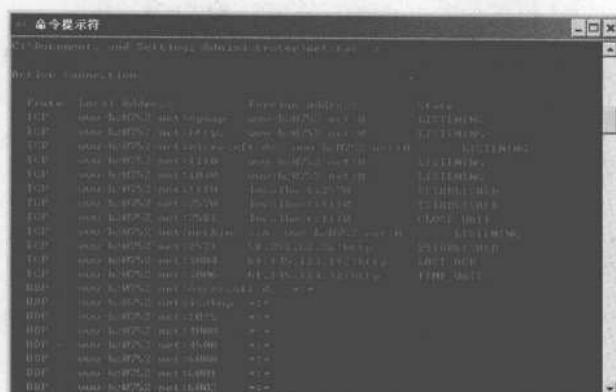
例：显示名为“\\WWW-HZ-0752-NET”的计算机的时间，如图1-36所示。



【图1-36】net time命令

8.netstat -a/-n

作用：-a参数获得机器当前的所有网络连接，包括当前用户的连接、其他用户的连接和系统进程的连接，如图1-37所示。



【图1-37】netstat的-a参数

9.netstat -b

作用：显示当前打开的端口正被那个应用程序所占用，如图1-38所示。



【图1-38】netstat的-b参数

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

10.netstat -r

作用：显示本机的路由表，如图1-39所示。



【图1-39】 netstat的-r参数

11.netstat -s

作用：按照各个协议分别显示其统计数据，如图1-40所示。



【图1-40】 netstat -s命令

12.netstat -n

作用：-n参数要求netstat不对IP地址进行DNS域名解析，即直接以IP地址的形式显示连接的机器，如图1-41所示。



【图1-41】 netstat -n命令

1.3.2 使用实战

【案例1-2】综合应用net命令建立入侵建立后门账号。

IPC\$本来主要是用来远程管理计算机的，但实际上往往被入侵者用来与远程主机实现通信和控制。入侵者能够利用它做到：建立、拷贝、删除远程计算机文件，在远程计算机上执行命令。

(1) 编写BAT文件。

打开记事本，键入“net user hackbak 123456 /add”和“net localgroup administrators sysback /add”命令，编写好命令后，把该文件另存为“hack.bat”。下面对这两个命令进行说明。

命令一：net user hackbak 123456 /add。该命令表示添加用户名为hackbak，密码为123456的账号。

命令二：net localgroup administrators sysback /add。该命令表示把hackbak添加到管理员组（administrators）。

(2) 与目标主机建立IPC\$连接。在上面的实例中已经介绍过这一步骤，所以这里省略。

(3) 拷贝文件至目标主机。

使用命令：copy FILE \\IP\PATH。“FILE”表示本地的文件名；“IP”为目标主机的IP地址；“PATH”保存文件的路径。

打开DOS命令行，键入“copy hack.bat \\192.168.27.128\c\$”命令copy命令执行成功后，就已经把D盘下的hack.bat文件拷贝到192.168.27.128的C盘内。此外，也可以在图形界面下把hack.bat复制、粘贴到目标主机中。

(4) 通过计划任务使远程主机执行hack.bat文件。

首先键入“net time \\IP”命令查看远程主机的系统时间，再键入“at \\IP TIME COMMAND”命令在远程主机上建立计划任务。

参数说明：

IP：目标主机IP

TIME：设定计划任务执行的时间

COMMAND：计划任务要执行的命令

打开DOS命令行，键入“net time \\192.168.27.128”命令。假设回显的目标系统时间为13:33，然后根据该时间为远程主机建立计划任务。键入“at\\192.168.27.128 13:45 c:\hack.bat”命令，该命令表示在下午13点45分执行目标主机C盘中的hack.bat文件。计划任务添加完毕后，使用命令“net use * /del”断开IPC\$连接。

【案例1-3】记住恶意骚扰的IP地址，以便投诉。

经常上网的人一般都使用QQ，有时候会被一些讨厌的陌生人骚扰，想投诉却又不知从何下手。其实，我们只要知道对方的IP，就可以向他所属的ISP投诉了。

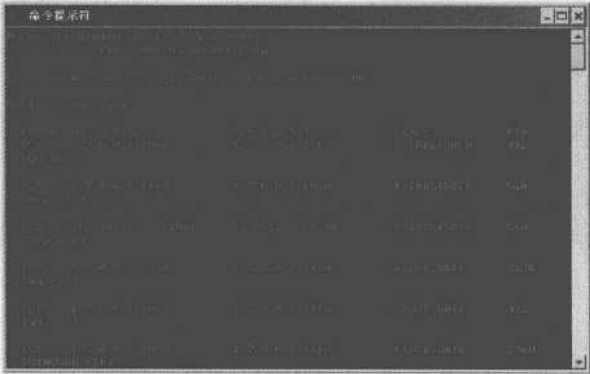
但怎样才能通过QQ知道对方的IP呢？一种方式是安装QQ的外挂或者显IP地址的版本，但即使是这样，由于各种原因，有时候也不能显示出对方的IP地址（特别是当对方隐身或通过服务器中转时）。

另一种方法是使用netstat命令，我们只需要通过netstat就可以很方便的做到这一点。

其操作步骤如下：

当他通过QQ或其他的工具与自己相连时（例如给他发一条信息或他给我们发一条信息），我们立刻在命令行输入界面下输入netstat -bn或netstat -ba就可以看到对方上网时所用的IP或ISP域名了，甚至连所用端口都完全暴露了。加参数-b的目的是显示当前打开的端口正被

哪个应用程序所占用，这样就方便我们确定QQ.exe程序占用的端口，也就容易找到对方目前所在的那个连接了。如图1-42所示，此时发送QQ消息的对方IP地址为：211.83.125.65。



【图1-42】定位QQ聊天对象的IP地址

netstat还经常用于网络流量的统计。有人使用netstat的-s和-e参数编写了一些统计软件，对计算机的网络接口进行24小时监控，并记录日志。如果发现某些时刻访问量特别大，并且全部是一些短小的TCP报文（例如大量很小的SYN报文），则机器很可能在这些时候受到了DOS攻击。还可以使用netstat -an命令记录下这些攻击的源地址，以便日后处理或投诉。

1.4 telnet和ftp命令

Telnet命令用于Internet的远程登录。它可以使用户坐在已上网的电脑键盘前通过网络进入的另一台已上网的电脑，使它们互相连通，这种连通可以发生在同一房间里面的电脑或是在世界各范围内已上网的电脑。习惯上来说，被连通计算机，并且为网络上所有用户提供服务的计算机称之为服务器（Servers），而自己在使用的机器称之为客户机（Customer）。一旦连通后，客户机可以享有服务器所提供的一切服务。用户可以运行通常的交互过程（注册进入，执行命令），也可以进入很多的特殊的服务器如寻找图书索引，网上不同的主机提供的各种服务都可以被使用。

FTP命令是Internet用户使用最频繁的命令之一，不论是在DOS还是UNIX操作系统下使用FTP，都会遇到大量的FTP内部命令。熟悉并灵活应用FTP的内部命令，可以大大方便使用者，并收到事半功倍之效。

1.4.1 使用方式图解

telnet命令的使用也是在telnet后面跟命令的参数。直接键入telnet，则进入telnet的命令行模式，如图1-43所示。在此命令行模式中，可以使用遵循telnet客户端规范的客户端命令和服务器进行互操作。



【图1-43】telnet的命令行模式

FTP命令的使用也是在FTP后面跟命令的参数。

命令格式：ftp [-v][-d][-i][-n][-g][-sfilename][-a][-wwindow size][computer]

- v 不显示远程服务器响应
- n 禁止第一次连接的时候自动登录
- i 在多个文件传输期间关闭交互提示
- d 允许调试、显示客户机和服务器之间传递的全部ftp命令
- g 不允许使用文件名通配符，文件名通配符的意思是说允许在本地文件以及路径名中使用通配字符

-sfilename 指定包含ftp命令的文本文件。在ftp命令启动后将自动运行这些命令。在加的参数里不能有空格。

- a 绑定数据连接时，使用的本地端口
- wwindow size 忽略默认的4096传输缓冲区

computer 指定要连接的远程计算机的ip地址

例：尝试连接IP地址为211.83.125.22的计算机，如图1-44所示，没有连接上，出现了错误，可能是对方未开机或者其他原因。



【图1-44】FTP的命令行模式

1.4.2 使用实战

【案例1-3】telnet到一台远程机器。

要telnet到一台远程机器，直接键入：telnet 机器域名（或IP地址）就可以了。例如，我们使用telnet登录四川大学BBS系统，已经知道四川大学BBS的机器域名为bbs.scu.edu.cn，要telnet登录四川大学BBS就只需要键入telnet bbs.scu.edu.cn，如图1-45所示。



端口是计算机网络层次结构中应用层和传输层通信的接口。一般来讲，一个端口标明应用层的一种服务。例如，HTTP服务的默认端口是80，FTP服务的默认端口是21。许多网络病毒和蠕虫都是攻击计算机的特定端口来潜入系统的。

如果telnet的目的端口不是运行着telnet服务的telnet服务器端口（默认是23端口），则telnet客户端就不可能得到正确的返回信息，所以可能出现黑屏等现象。但这并不影响我们测试目的机器端口的通断。只要返回的不是“Could not open connection to the host”，则一定表明该端口是打开的。

【案例1-5】利用FTP命令连接目标计算机。

连接一个ftp服务器（例如ftp.tsinghua.edu.cn），只需要键入：ftp ftp.tsinghua.edu.cn
然后根据提示输入用户名、密码等信息就可以了，如图1-48所示。

```
C:\Documents and Settings\Administrator\Desktop>ftp ftp.tsinghua.edu.cn
Connected to ftp.tsinghua.edu.cn.
220 FTP Service at Tsinghua University.
User (ftp.tsinghua.edu.cn:root) root:
root
270
271
272
273
274
275
276
277
278
279
280
```

【图1-48】使用ftp命令连接ftp服务器

1.5 tracert命令

tracert命令是一个诊断程序，该诊断实用程序将包含不同生存时间（TTL）值的 Internet 控制消息协议（ICMP）回显数据包发送到目标，以决定从一个主机到网络上其它主机的路由。

如果有网络连通性问题，可以使用tracert命令（tracert命令是英文单词“trace route”的缩写，意思是跟踪路径）来检查到达目标IP地址的路径并记录结果。

Tracert 工作原理：

每个路由器要在转发数据包上的TTL之前至少递减1，必需路径上的每个路由器，所以TTL是有效的跃点计数。数据包上的TTL到达0时，路由器应该将“ICMP 已超时”的消息发送回源系统。Tracert 先发送 TTL 为 1 的回显数据包，并在随后的每次发送过程将 TTL 递增1，直到目标响应或 TTL 达到最大值，从而确定路由。路由通过检查中级路由器发送回的“ICMP 已超时”的消息来确定路由。



TTL (Time to Live) 的意思是存在时间值，通过该值可以算出数据包经过了多少个路由器，方法是：用255减去返回的TTL值，例如本例中返回250，则应该用255来减去250，得到5。

1.5.1 使用方式图解

tracert的使用很简单，和ping命令相同，只需要在tracert一个IP地址或域名。如果跟域名，tracert会自动进行相应的域名转换。

Tracert 命令支持多种选项，如下：

- (1) tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
- (2) -d 指定不将 IP 地址解析到主机名称。
- (3) -h maximum_hops 指定跃点数以跟踪到称为 target_name 的主机的路由。
- (4) -j host-list 指定 Tracert 实用程序数据包所采用路径中的路由器接口列表。
- (5) -w timeout 等待 timeout 为每次回复所指定的毫秒数。
- (6) -target_name 目标主机的名称或 IP 地址。

例：使用tracert 观察本机到www.scu.edu.cn经过的路径，如图1-49所示。www.scu.edu.cn的IP地址就是202.115.32.61。



【图1-49】tracert命令



ICMP是网络报文控制协议的缩写，主要用于协助IP通信报文进行差错控制和检测。ping和tracert命令都是使用ICMP协议的通信原理来获得信息的。笔者自己开发了一个图形界面的ping和tracert实用程序，并将源代码附在本书光盘中供读者使用和研究。

除了在本章1.2.2节中学到的使用“ping远程服务器域名”命令来实现域名对IP地址的转换功能，还可以用本节中介绍的“tracert远程服务器域名”命令来实现域名对IP地址的转换功能。

1.5.2 使用实战

Tracert一般用来检测故障的位置。如果某台计算机不能ping通，可能是中间网络故障所致。这时可以用tracert命令检测通信路径上是哪个环节上出了问题，如果tracert失败，可以使用命令输出来帮助确定哪个中介路由器转发失败或耗时太多，为解决问题指出方向。

【案例1-6】举例实际分析tracert命令输出，操作步骤如下：

本例中，数据包必须通过两个路由器（10.0.0.1 和 192.168.0.1）才能到达主机 172.16.0.99。主机的默认网关是 10.0.0.1，192.168.0.0 网络上的路由器的 IP 地址是 192.168.0.1。键入tracert 172.16.0.99 -d命令后显示结果如下：

```
C:\>tracert 172.16.0.99 -d
Tracing route to 172.16.0.99 over a maximum of 30 hops
 1 2s 3s 2s 10, 0.0, 1
 2 75 ms 83 ms 88 ms 192.168.0.1
 3 73 ms 79 ms 93 ms 172.16.0.99
Trace complete.
```

【案例1-7】使用tracert命令确定数据包在网络上的停止位置，其操作步骤如下：

本例中，默认网关确定 192.168.10.99 主机没有有效路径。这可能是路由器配置的问题，或者是 192.168.10.0 网络不存在（错误的 IP 地址）。键入命令tracert 192.168.10.99后显示结果如下：

```
C:\>tracert 192.168.10.99
Tracing route to 192.168.10.99 over a maximum of 30 hops
 1 10.0.0.1 reports:Destination net unreachable.
Trace complete.
```

1.6 ipconfig命令

ipconfig命令主要用来显示当前系统的TCP/IP配置。

1.6.1 使用方式图解

直接键入ipconfig，可以显示机器当前的IP地址，子网掩码和网关IP，如图1-50所示。“IP Address”是机器当前的IP地址。“Subnet Mask”是子网掩码，“Default Gateway”是默认网关的IP。



【图1-50】使用ipconfig命令获得TCP/IP配置信息

1.6.2 使用实战

【案例1-8】用ipconfig命令获知计算机的MAC地址。

键入ipconfig /all 则显示出更多额外信息，如图1-51所示。现在利用ipconfig /all获得计算机的MAC地址、网卡名、DNS设置，获得MAC地址十分有用。当IP地址变化时MAC地址时唯一的，能标志计算机。



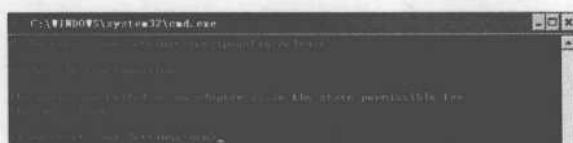
【图1-51】ipconfig的/all参数

在『例子1-8』中，计算机的MAC地址是00-14-2A-9D-0E-CD，使用“Uia PCI 10/100Mb Fast Ethernet Adapter”型号的网卡，DNS设置为“61.139.2.69”。

【案例1-9】判断是否向DHCP服务器租用IP地址。

ipconfig /release和ipconfig /renew这是两个附加选项，只能在向DHCP服务器租用IP地址的计算机上起作用，在非DHCP服务器的计算机上会显示如图1-52所示的信息，这样来判断使用的计算机是否通过DHCP服务器租用IP地址。

如果输入ipconfig /release，那么所有接口的租用IP地址便重新交付给DHCP服务器（归还IP地址）。如果我们输入ipconfig /renew，那么本地计算机便会设法与DHCP服务器取得联系，并租用一个IP地址。请注意，大多数情况下网卡将被重新赋予和以前相同的IP地址。如图1-53所示。



【图1-52】非DHCP服务器的计算机



【图1-53】ipconfig的/release和/renew参数

1.7 route命令

route命令顾名思义，是和路由有关的命令。它主要用来显示当前主机中的路由信息。如果需要改变和删除一些路由项，也要使用route命令。

1.7.1 使用方式图解

route命令的使用也是在route后面跟参数。直接键入route，然后回车，就会出现如图1-54所示的所有参数和语法。



【图1-54】route命令的参数和语法

route print 命令用于显示系统的选路表，如图1-55所示。



【图1-55】 route print命令

1.7.2 使用实战

【案例1-10】使用route add命令添加静态路由。

例如，要添加一条到157.0.0.0/8，下一条是157.55.80.1，从接口“本地连接”转发的静态表项，应键入如下命令：

route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF “本地连接”，显示如图1-56所示。



【图1-56】 添加静态路由

【案例1-11】使用route delete命令删除一条路由表项。

操作步骤如图1-57所示。



【图1-57】 删除一条路由表项

【案例1-12】route change命令更新已有的路由表项。

操作步骤如图1-58所示。



【图1-58】 更新已有的路由表项

注意：netstat r和route print命令功能基本是一样的。因此，查看系统的选路表也可以用netstat -r命令代替。

1.8 netsh命令

netsh命令是一个复杂的综合网络设置工具，是本地或远程计算机的Windows2000网络组件的命令行和脚本实用程序。为了存档或配置其他服务器，netsh实用程序也可以将配置脚本保存在文本文件中。

netsh 实用程序是一个外壳，它通过附加的“Netsh帮助DLL”，可以支持多个Windows 2000组件。“netsh帮助DLL”提供用来监视或配置特定Windows2000网络组件的其他命令，从而扩展了netsh的功能。每个“netsh帮助DLL”都为特定的网络组件提供了一个环境和一组命令。每个环境中都可以有子环境。例如，在路由环境中存在子环境Ip和Ipx，它们将IP路由和IPX路由命令集中在一起。

1.8.1 使用方式图解

netsh有自己的命令行接口（CLI），直接键入netsh就进入netsh的命令行接口，如图1-59所示。netsh接口采用目录树的命令组织方式，将大多命令以树节点的方式组织起来。要访问interface命令节点，直接在根下面键入interface。要返回上级目录，则键入“.”号。



【图1-59】 netsh的命令行接口

1.8.2 使用实战

netsh可以设置几乎所有的主机网络相关配置。这里使用netsh配置网卡IP地址，网络掩码，网关地址和DNS服务器信息。

『案例1-13』使用netsh配置网卡IP地址，网络掩码，网关地址和DNS服务器信息。
下表列出了主机需要配置的TCP/IP信息：

主机需要配置的TCP/IP信息	
IP地址	211.83.125.65
子网掩码	255.255.254.0
网关地址	211.83.125.254
网关跳数	1
获取IP地址方式	静态获取
DNS服务器地址	202.112.14.151

打开DOS命令行，配置过程如图1-60所示。



【图1-60】使用net命令配置主机TCP/IP信息

注意：配置完毕后，可以立即使用dump命令查看当前配置。

1.9 arp命令

arp命令用于显示和设置系统的物理地址表（ARP Table）中的信息，也是功能强大、比较常用的命令。

1.9.1 使用方式图解

arp命令的使用也是在arp后跟命名的参数，直接键入arp后回车将显示arp命令的所有的语法，如图1-61所示。



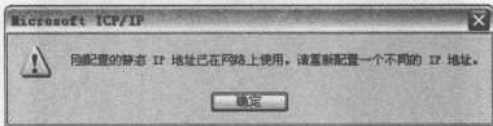
【图1-61】arp命令

键入arp -a显示系统MAC表中的记录，如图1-62所示。



【图1-62】arp命令的-a参数

在局域网中，如果使用一个已经被别人占用的IP地址，则配置网卡时，Windows操作系统将弹出一个对话框，提示刚配置的静态IP地址已经被网络上其他计算机占用，即不允许我们使用该IP地址，如图1-65所示。



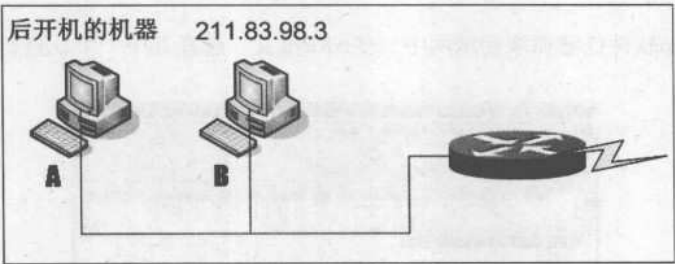
【图1-65】Windows操作系统不允许使用已被占用的IP

事实上，在静态配置IP地址的局域网内，对于同样一个IP地址，谁先开机，谁就有优先使用的权利；后开机的机器可以通过攻击手段抢占IP地址。在图11-1-2所构造的网络中，后开机的计算机（A机）不断发送伪造的ARP报文，使路由器的ARP记录指向A；而先开机的计算机（B机）长期不能获得路由器的转发服务，也就不能上网，这样B机的用户就会考虑更换其IP地址。当B机更换IP地址后，A机便可以合法使用B机以前的IP，达到抢占IP的目的。

接下来，我们综合利用Sniffer Pro软件和命令行方式下的arp、ping等命令来学习如何在局域网中抢占IP。

(1) 搭建试验环境

先来搭建一个试验环境，如图1-66所示，假设局域网网段范围211.83.98.0—211.83.98.127，网关路由器的IP地址为211.83.98.1。网络中已经有一台计算机使用IP为“211.83.98.3”的地址。我们的计算机后开机，不能将IP地址设置为211.83.98.3。



【图1-66】构造抢占IP地址的试验环境

(2) 记录本机（计算机A）的MAC地址

在cmd.exe命令行模式下，输入命令ipconfig /all，记录本机MAC地址为“50-78-4C-6B-28-D3”。

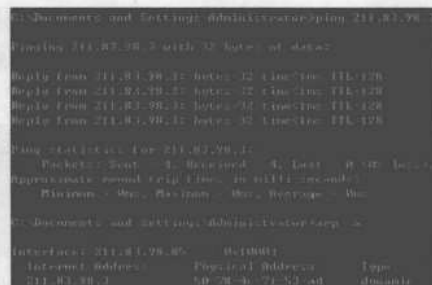
(3) 记录计算机B的MAC地址

在cmd.exe命令行模式下，输入命令：

ping 211.83.98.3

arp -a

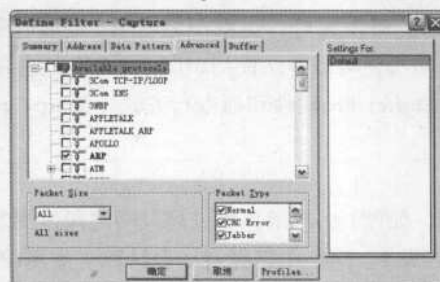
获得IP地址为211.83.98.3的计算机的MAC地址为“50-78-4c-71-53-ad”，如图1-67所示。



【图1-67】获取机器211.83.98.3的MAC地址

(4) 使用Sniffer Pro软件产生ARP欺骗报文

首先将Sniffer Pro的抓包过滤器设置为只抓取ARP报文，如图1-68所示。



【图1-68】设置Sniffer Pro的抓包过滤器只抓取ARP报文

用Sniffer Pro软件任意抓取局域网中一些ARP报文，选择其中一个，进行解码分析，如图1-69所示。



【图1-69】解码分析任意一个ARP报文

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

ARP报文分为ARP请求和ARP响应。在图1-69中容易看到ARP报文格式中包含源/目的物理地址字段，源/目的IP地址字段。这四个字段在ARP报文中的具体位置如下所示：

四字段在ARP报文中的位置	
地址	所在位置（从报文头开始的字节）
源物理地址	23—28
源IP地址	29—32
源物理地址	33—38
源物理地址	39—42

正是要修改这四个字段，达到欺骗路由器的目的。

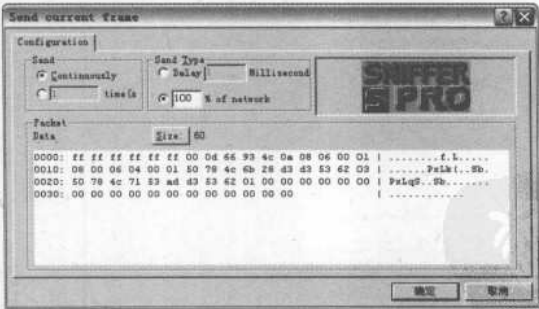
在解码窗口中选择的ARP报文上单击鼠标右键，选择“Send Current Frame”。弹出“Send current frame”窗口。改变该ARP报文的四个地址字段的值，构造如图1-70所示的ARP报文。

```
0000: ff ff ff ff ff ff 00 0d 66 93 4c 0a 08 06 00 01 | .....f.L....
0010: 08 00 06 04 00 01 50 78 4c 6b 28 d3 53 62 03 | .....Pxlk(..Sb.
0020: 50 78 4c 71 53 ad d3 53 62 01 00 00 00 00 00 | PxlqS..Sb.....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
```

【图1-70】构造新的ARP报文

注意：图1-70中，“d3 53 62 03”是源IP地址“211.83.98.3”的16进制表示。“d3 53 62 01”是目的IP地址“211.83.98.1”的16进制表示。

在“Send current frame”窗口中选择“Send”方式为“Continuously”，“Send Type”是“100% of network”，单击确定开始产生ARP欺骗报文，如图1-71所示。



【图1-71】产生ARP欺骗报文

(5) 将本机（计算机A）的IP修改为计算机B的IP

第四步执行之后，计算机B已经不能正常上网了。由于选择了“Continuously”模式，很可能导致计算机B直接死机（对计算机B的破坏相当严重）。Sniffer Pro发送一段时间后，将本机IP修改为计算机B的IP，就完成抢占IP地址的全部工作了。

1.10 小结

本章简单介绍了DOS操作系统的原理，以及WindowsNT/2000/XP平台下使用DOS命令的方法，然后着重介绍了八个常用的和网络相关的DOS命令的用法。这些命令对于黑客来说是发现攻击对象和发动攻击最好的工具，而对于普通用户来说是管理计算机网络和排除网络故障的工具。从另一方面来说，熟练掌握了这些命令也就明白了黑客进攻的途径，从而可以做好防范工作。

本章介绍的这些黑客常用命令对于一个想要成为黑客的人来说是必须熟练掌握的，读者对这些命令感兴趣的话可以先在自己的计算机上操练，切不可随意攻击别人的计算机，被发现后很有可能被举报。这些命令是黑客常用命令，同时也是常用的检查网络和计算机状态的命令，所以，熟练掌握之后对提高计算机操作技能和排除故障的能力也大有裨益。

第2章 扫描及端口扫描工具

在学习了常用黑客命令之后，就可以开始学习黑客技术的核心——扫描技术了！因为黑客首先要通过扫描，确定某台计算机作为攻击对象，然后通过扫描探测发现这台计算机主机的漏洞，才可能对此漏洞展开攻击，扫描的重要性显而易见。在学习扫描工具之前，先介绍一些网络的基本知识，包括IP地址的概念、分类等，然后再介绍IP地址的定位技术和针对定位技术的IP隐藏技术。最后，本章为读者介绍了端口基本知识和端口安全措施。

本章要点

- ◎ IP地址及其作用
- ◎ IP扫描的原理以及应用
- ◎ IP隐藏保护的方法
- ◎ 端口扫描的原理
- ◎ 常用重要端口

2.1 IP地址的查找及锁定

IP地址的概念、分类和作用为基础的知识，在此不表，我们现在重点学习如何对IP地址进行查找以及锁定。

2.1.1 由网址查找IP

访问网站的时候，往往敲入的不是IP地址，而是网站的网址。网址其实就是机器的域名，它与IP地址不同，有具体的含义，也便于书写和记忆。但在IP选路的过程中，网址需要通过DNS服务器中的记录映射成为IP地址。如果知道对方的IP地址，就容易查出对方的ISP、地理位置等信息；黑客也容易采取一定手段进行IP攻击。如何由网址查找出IP地址呢？可以利用网络上大量的DNS服务器提供的正向查询功能。在第一章中，我们曾经提到过使用ping命令或是tracert命令间接进行DNS查询。

本小节讨论Windows系统提供的真正的DNS客户端查询软件：nslookup。

【案例2-4】使用nslookup查询IP地址。

(1) 打开命令行输入界面，输入nslookup，进入nslookup命令的命令模式。nslookup首先返回当前系统设置的DNS服务器信息。DNS服务器的名字是ns.sc.cninfo.net，IP是61.139.2.69，如图2-1所示。



【图2-1】命令行运行nslookup命令

(2) 要查询一个网址对应的IP地址（例如网易www.163.com.），只需要输入www.163.com就可以了。



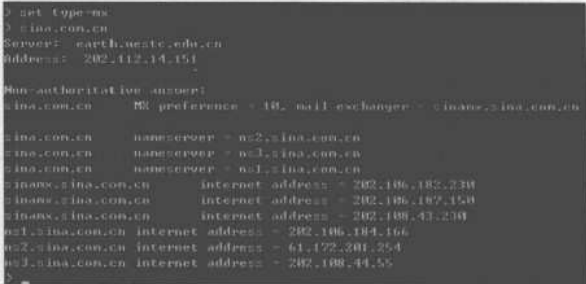
【图2-2】www.163.com.cn对应的IP地址

在图2-18中，nslookup查到一条DNS的A记录：www.163.com的IP地址是220.181.28.51\220.181.28.52\220.181.28.53\220.181.28.54\220.181.28.205\220.181.28.206\220.181.31.182\220.181.31.183\220.181.31.184\220.181.28.50（这几个IP地址都是）。

(3) nslookup默认查询的是A记录。如果要查询其他记录，可以使用set type=××这条命令。例如，要查询sina.com.cn的MX记录，只需要输入两行命令：

```
set type = mx
sina.com.cn
```

就可以了，如图2-3所示。



【图2-3】查询sina.com.cn的MX记录



DNS服务器上记录的数据称为“资源记录（RR）”。资源记录有许多不同类型，如A记录、MX记录、NS记录、PTR记录、CNAME记录、AAAA记录、TEXT记录等等。最常用和最重要的是A记录，它为DNS客户端正向查询提供信息，帮助客户端从机器名称返回对应的IP地址。MX记录与邮件交换服务器有关；NS记录反映了一个DNS域中DNS服务器的名字和地址；而PTR记录用做从IP地址到机器域名的反向查询。

2.1.2 查找电子邮件发送者IP

目前电子邮件的发送遵循SMTP协议，而许多邮件服务器允许用POP3协议通过客户端软件（Outlook、Foxmail）等接收邮件。

有时电脑会收到许多垃圾邮件。有时则收到一些带病毒附件的邮件，只要打开这些附件，计算机就可能立即中毒，出现死机、蓝屏等现象，或是打开后门程序使机器被黑客控制。这些都是不愉快的事情，我们希望查到元凶是谁，即有没有办法知道邮件最初是从哪个IP地址发送到网络上的呢？其实只要能将邮件接收到自己的电脑中，就一定能够找出发件人的IP。

【案例2-5】使用以Foxmail客户端查找邮件发送者IP。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

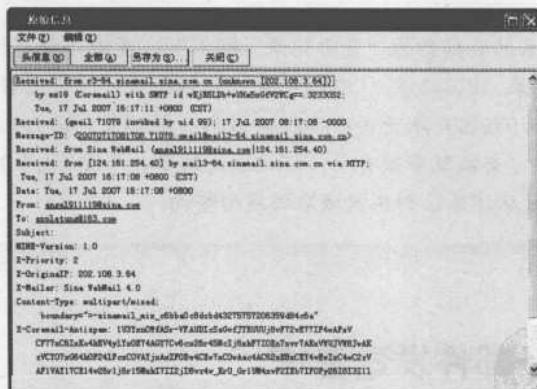
黑客
兵器大曝光

(1) 打开要处理的邮件，单击“邮件”→“邮件信息”→“查看原始信息”，如图2-4所示。



【图2-4】用Foxmail查看邮件原始信息

(2) 打开“原始信息”对话框后，邮件头的源代码就出现了。注意第一个“Received From”后的机器名和IP地址就是这封电子邮件发件人的机器名和IP地址。如图2-21所举例子中的邮件是由叫“r3-64.sinamail.sina.com.cn”的机器发出的，而这台机器的IP地址是“202.108.3.64”。



【图2-5】通过Foxmail找出发件人的IP

2.1.3 查找远程局域网用户的IP

【案例2-6】使用LanSee查找远程局域网用户的IP。

局域网查看工具（LanSee）采用多线程技术，搜索速度很快。它将局域网上比较实用的功能完美地融合在一起，比如搜索计算机（包括计算机名，IP地址，MAC地址，所在工作组，用户），搜索共享资源，搜索共享文件，多线程复制文件（支持断点传输），发短消息，高速端

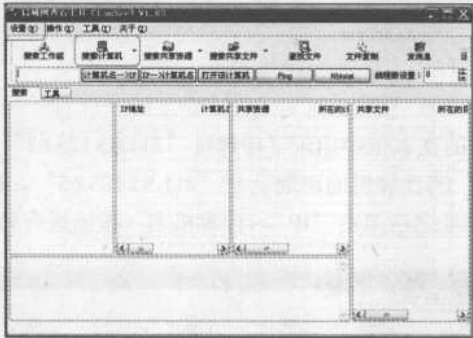
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 2 章 IP 及端口扫描工具

口扫描，捕获指定计算机上的数据包，查看本地计算机上活动的端口，远程重启/关闭计算机等，功能十分强大。该软件是一款绿色软件，解压后直接打开运行，无需安装。

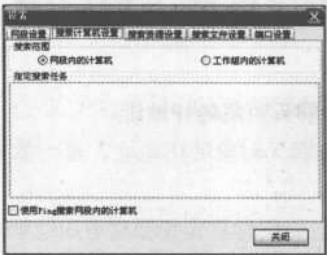
使用LanSee查找远程局域网用户的IP具体步骤如下：

(1) 打开LanSee主界面，在菜单栏中单击“设置”菜单，如图2-6所示。



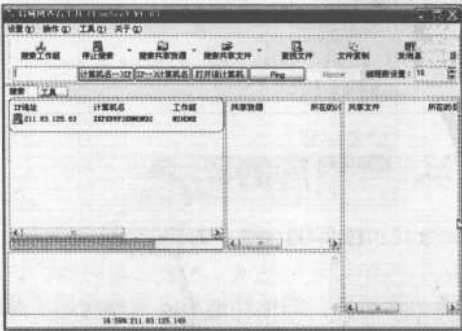
【图2-6】LanSee主界面

(2) 在弹出的“设置”对话框中可以设置扫描的范围等，设置好之后单击“关闭”按钮，如图2-7所示。



【图2-7】“设置”对话框

(3) 回到主界面中，单击工具栏里的“搜索计算机”图标，开始搜索，并显示搜索的进程和搜索到的计算机名、工作组、IP地址、MAC地址等信息，如图2-8所示。

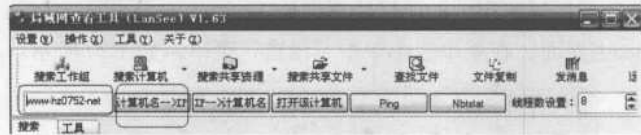


【图2-8】搜索的进程和结果

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

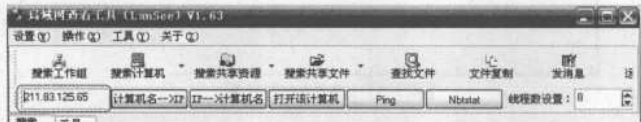


(4) 如果已知局域网内一个计算机名要查它的IP地址则在工具栏下方的文本框中输入计算机名，例如“www-hz-0752-net”，然后单击“计算机名-->IP地址”按钮，如图2-9所示。



【图2-9】根据计算机名要查IP地址

(5) 刚才输入计算机名的文本框中出现了IP地址“211.83.125.65”，如图2-10所示。说明这台名为“www-hz-0752-net”的计算机的IP地址是“211.83.125.65”。已知IP地址要查计算机名也是同样的道理，输入IP地址之后单击“IP-->计算机名”按钮进行转换。



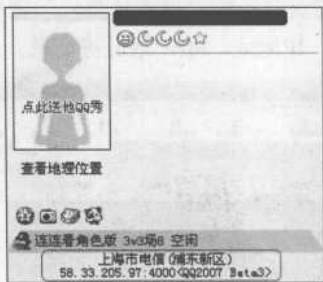
【图2-10】显示计算机的IP地址

2.1.4 用珊瑚虫版QQ了解聊天用户IP

「案例2-7」使用珊瑚虫版QQ聊天对象的IP地址。

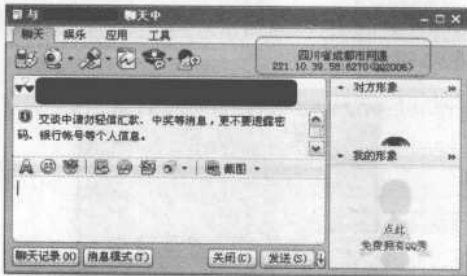
珊瑚虫版QQ可以显示自己和聊天对象的IP地址，是一款方便地得到聊天用户IP地址的软件。操作步骤如下：

(1) 使用珊瑚虫版QQ登录，将鼠标移到想要察看IP地址的好友头像上，在旁边就会出现如图2-11所示的显示状态栏，显示出好友的所在的城市和IP地址。这个方法在好友在线的时候才能使用，如果好友处于隐身状态就需要和他发送信息了。



【图2-11】查看在线好友IP地址

(2) 向隐身的好友发送一条信息，当他回信息之后就变成了在线状态，此时，在聊天对话框的右上角就会出现好友的城市和IP地址了，如图2-12所示。



【图2-12】查看隐身好友IP地址

2.1.5 用IP地址定位器定位真实地理地址

用IP地址定位器运行在windows平台下的IRC软件里。利用本软件可以找出irc聊天室中一个NICK具体地理位置（城市级别），并且作为一个小窗的消息显示出来。

【案例2-8】用IP地址定位器定位真实地理地址。

IP地址定位器可以用来定位任意一个IP地址的真实地理位置，不用对IRC的脚本做任何改变，全部由安装程序完成。使用IP地址定位器定位真实地理地址具体步骤如下：

(1) 安装IP地址查找器，然后打开此程序，弹出“IP地址查找器V2.0的主界面”，如图2-13所示。



【图2-13】IP地址定位器主界面

(2) 在“要查找的IP地址”栏中输入“202.115.104.*”，然后单击“查找”按钮，如图2-14所示。

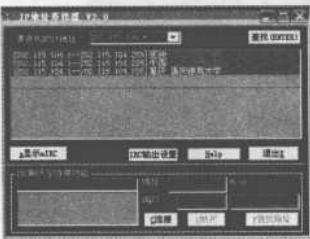


【图2-14】输入要查找的IP地址

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



(3) 开始查找，查找结果显示在状态栏中，此IP地址的地理位置是“亚洲，中国，重庆，重庆建筑大学”，如图2-15所示。



【图2-15】查找结果

2.2 IP扫描

IP扫描工具通过截获和分析IP数据包进行IP地址获取、网关获取、子网大小探索、MAC地址获取、端口扫描等扫描活动。本节将介绍几种典型的IP扫描工具，希望对这类工具的使用起到抛砖引玉的作用。

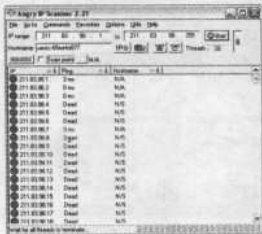
2.2.1使用Angry IP Scanner检测IP动态

【案例2-9】使用Angry IP Scanner检测IP动态

Angry IP Scanner是一个小巧的IP扫描软件，不过虽然体积小，功能却一点也不少，可以在最短的时间内扫描远端主机IP的运作状况，快速整理结果并回报给本机用户知晓。Angry IP Scanner可以扫描的项目比较多，包括了远端主机的名称、当前开启的共享服务以及IP的运作状况等，用户完全可以掌握对方主机的运作状况。Angry IP Scanner可以允许扫描的范围相当大，只要不嫌花费的时间比较长，可以从1.1.1.1一直扫到255.255.255.255，AngryIP Scanner会详实地ping每个IP，并且将状态及时返回给用户。

Angry IP Scanner很容易上手，下面具体介绍Angry IP Scanner的用法。

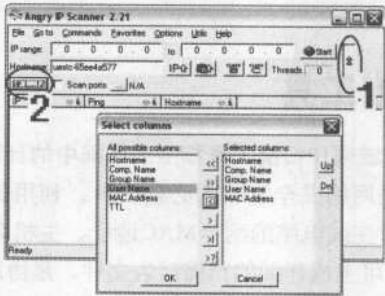
(1) 在主界面上输入要扫描的IP范围，单击“Start”就可以开始扫描了。图2-16中Angry IP Scanner正在扫描网段“211.83.98.1-255”所有机器。机器列表中蓝色表示该机器响应ping报文；红色表示超时。



【图2-16】利用Angry IP Scanner扫描网段内的机器

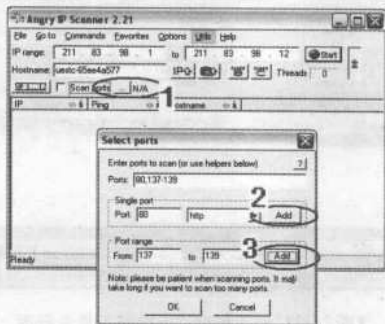
第 2 章 IP 及端口扫描工具

(2) Angry IP Scanner 可以通过扫描 IP 获取更多信息。依次单击图 2-17 中所示 1 和 2 处，弹出“Select columns”对话框，选择需要进一步获取的信息。



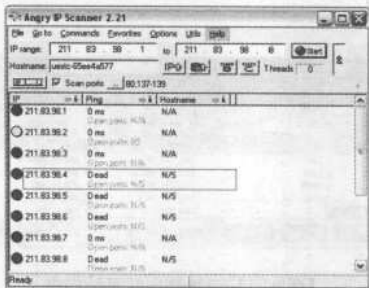
【图 2-17】通过 Angry IP Scanner 扫描 IP 获取更多信息

(3) Angry IP Scanner 还可以进行端口扫描。在图 2-18 中单击图中所示 1 处，弹出“Select ports”对话框。可以通过“Single port”输入单个需要扫描的端口，并单击 2 处的“Add”；也可以通过“Port range”输入需要扫描的端口范围，并单击 3 处的“Add”。本例中将要扫描的端口定为 80 端口、137 端口—139 端口共四个端口。



【图 2-18】设置 Angry IP Scanner 进行端口扫描

(4) 设置端口后，在 IP 扫描的同时，Angry IP Scanner 也进行端口扫描。图 2-19 的例子显示了机器 211.83.98.2 的 80 端口是处于开启状态的。



【图 2-19】利用 Angry IP Scanner 进行端口扫描

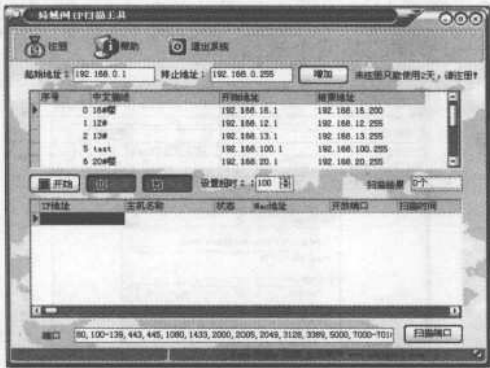
注意：Angry IP Scanner采用了多线程扫描机制提高扫描速度，一次性扫描几千台机器，几分钟就能完成。但如果待扫描的IP地址范围很大，而且又需要扫描很多端口，则可能会等待很长的时间。

2.2.2局域网IP扫描工具

【案例2-10】使用长天局域网IP扫描工具扫描局域网中的计算机。

长天局域网IP扫描工具是网络安全管理的必备工具，利用长天局域网IP扫描工具，可以远程扫描局域网内各个网段的在线电脑的网卡MAC地址、主机名称，进行端口扫描等各种信息，可以查出开放的端口号，可生成详细的扫描报告文件。是协助网管的好工具。长天局域网IP扫描工具使用步骤如下：

(1) 安装长天局域网IP扫描工具，然后打开此程序，弹出长天局域网IP扫描工具主界面，如图2-20所示。此工具分为上下两部分，上面部分是设置，下面空白处则用来显示扫描的机器的信息。



【图2-20】长天局域网IP扫描工具主界面

(2) 在“起始地址”栏和“终止地址”栏设置好需要扫描的网段，然后单击“增加”按钮，刚才增加的网段出现在表格中，如图2-21所示。选中此网段，单击“开始”按钮扫描，扫描结果将出现在图2-36中的下半部分空白中，包括IP 地址、主机名称、状态、MAC地址、开放端口、扫描时间几个信息。



【图2-21】设置网段并开始扫描

2.3 IP 隐藏保护

在本章的开头已经讲过黑客入侵的途径通常都要首先探测到一台计算机的 IP 地址，然后再发动攻击，所以保证计算机安全，防止黑客入侵的一个重要环节就是要隐藏好自己的 IP 地址，这样，黑客就不能把这台计算机作为攻击目标了。

IP 隐藏技术是通过动态 IP、代理 IP 或者 NAT 等技术将本机 IP 隐藏起来的专门技术。通过 IP 隐藏不仅可以保护自己的隐私，还可以保护机器不被互联网上 IP 扫描软件发现，使本机受 IP 攻击的可能性大为减小。

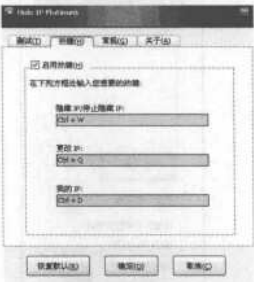
2.3.1 用 Hide IP Platinum 隐藏你的真实 IP

【案例 2-11】使用 Hide IP Platinum 隐藏真实 IP 地址。

- (1) 安装 Hide IP Platinum，然后打开此程序会弹出主界面，如图 2-22 所示。
- (2) 单击主界面中的“热键”按钮，弹出热键设置界面，可以选择功能的热键，选择好之后单击“确定”按钮，也可以单击“恢复默认”来恢复到默认的热键，如图 2-23 所示。



【图 2-22】Hide IP Platinum 主界面



【图 2-23】热键设置

- (3) 单击主界面中的“常规”按钮，选择语言和风格，然后单击“确定”按钮，如图 2-24 所示。
- (4) 隐藏 IP 运行标志显示在状态栏的右下角，用右键单击此标志，弹出菜单，可以选择“停止隐藏 IP”、“选项”、“退出”等选项，如图 2-25 所示。



【图 2-24】常规设置



【图 2-25】控制

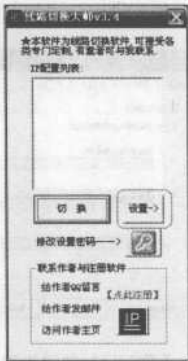
2.3.2 用“IP地址随意换”自由切换IP

【案例2-12】使用“IP地址随意换”自由切换IP。

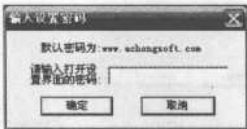
是否在来回更改IP配置而苦恼？是否希望能快速更改IP配置而不用重新启动系统？是否想通过密码设置来禁止他人修改配置信息？如果是的话，就请选择“IP地址随意换”（线路切换大师）吧！IP地址随意换（线路切换大师）是一款简易、实用、功能强大的IP切换工具，它可以帮助你预先设定的多个IP配置中自由地切换，可以添加、删除、修改原有的IP配置，可以自动获取和保存IP配置，可以设置密码来防止他人修改配置信息，可以设置开机自启，可以设置切换成功后自动退出，可以实现界面动态扩展和收缩等。

使用IP地址随意换的具体步骤如下：

- （1）打开“IP地址随意换”，弹出主界面，如图2-26所示。
- （2）弹出“输入设置密码”对话框，并且告知了默认的初始密码。输入此密码，然后单击“确定”按钮，如图2-27所示。



【图2-26】“线路切换大师”主界面



【图2-27】输入设置密码

- （3）弹出IP地址随意换主界面，单击“添加”按钮，如图2-28所示。

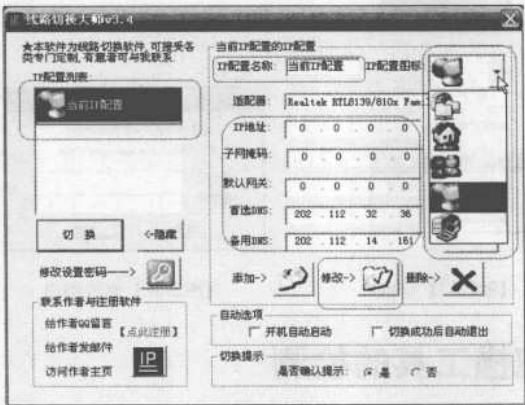


【图2-28】添加一个配置

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

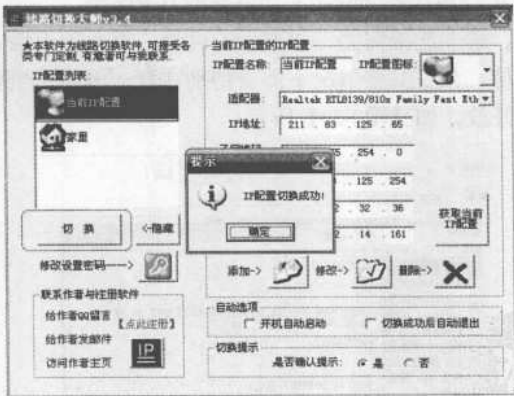
第 2 章 IP 及端口扫描工具

(4) 刚才添加的配置出现在主界面左上方的空白栏中，可以通过右上角的“IP配置名称”、“IP配置图标”和“IP地址”、“子网掩码”等来对新添加的IP配置进行设置，设置之后单击“修改”按钮来保存设置，如图2-29所示。



【图2-29】为“当前IP配置”设置配置

(5) 按照上述方法再添加一个名为“家里”的配置，这样就有两个配置了，如图2-30所示。选中“当前IP配置”图标，然后单击“切换”按钮，弹出“提示”对话框显示IP配置切换成功，现在使用的就是“当前IP配置”中设置的IP地址。

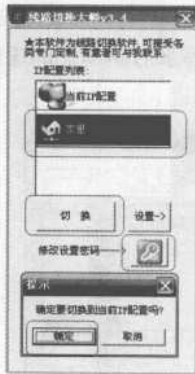


【图2-30】切换到“当前配置”

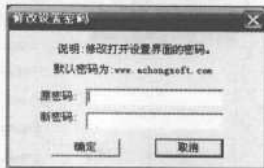
(6) 如果在公司里使用的IP是“当前IP配置”的IP，回家之后使用“家里”配置，那么从公司回家就可以打开“IP地址随意换”，选中“家里”图标，然后单击“切换”按钮，弹出“提示”对话框询问是否切换到此配置，单击“确定”按钮进行切换就可以了，如图2-31所示。

(7) 不希望别人随意使用“IP地址随意换”切换IP，可以为它重新修改密码，单击图2-31中的“修改设置密码”图标，弹出“修改设置密码”对话框，在此对话框中输入原密码和新密码，然后单击“确定”按钮就可以了，如图2-32所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图2-31】切换IP



【图2-32】修改密码

2.3.3 干扰IP扫描工具的检测

IP扫描工具通过截获和分析IP报文扫描远程机器中的信息，比如主机名、开放的端口、网卡物理地址等。IP扫描工具的工作原理一般是通过和目的主机建立TCP连接以获取各种信息。针对IP扫描工具的工作原理，我们提出两种干扰IP扫描工具的有效手段。

『案例2-13』使用防火墙。

配置用户防火墙，阻止一切从外部网络主动发起的TCP连接。

由于TCP是双向连接，建立连接需要三次握手的过程，因此防火墙并不会影响用户正常的主动向外部网络发起的通信。但在某些情况下需要特别注意，例如本机要开设一些网络服务，则必须要求相应端口对外开放，如【图2-33】所示。



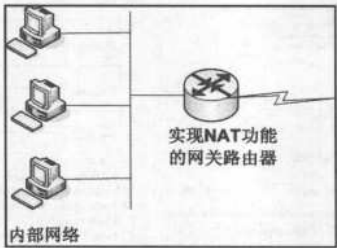
【图2-33】在Windows防火墙中开放FTP端口

『案例2-14』使用仿真IP。

所谓仿真IP，是指不使用Internet的全球唯一IP地址，而是使用一些保留的内部IP，通过地

址转换的方式实现IP仿真。使用仿真IP是干扰IP扫描工具的好办法。

对于局域网中的电脑，可以使用内部地址，然后利用NAT（网络地址转换）技术通过网关路由器访问外网，如图2-34所示。互联网上的计算机和内部网络的机器通信时，看到的IP地址是网关的IP而不是内部机器的IP。NAT技术的使用不仅隐藏了内部网络机器的IP地址，还能节约大量的外网地址。内部网络的机器一定程度上将网络安全工作交给有经验的网管人员，网管人员依靠网关路由器上防火墙的正确配置保障内部网络与Internet通信的安全。



【图2-34】典型的NAT应用拓扑图

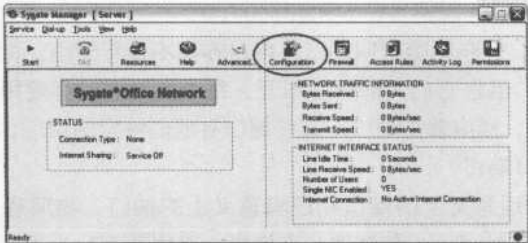
通常，NAT功能会被集成到路由器、防火墙、无线AP、或者单独的NAT设备中。用户只要购买了这些网络设备，就可以免费享用NAT技术带来的网络安全了。NAT设备维护一个状态表，用来把内部网络的IP地址映射到合法的外部IP地址上去。每个数据包在NAT设备中都被翻译成正确的IP地址，然后再发往下一级设备。

如果网关设备只有一个合法的外网IP，要实现仿真IP，需要使用一种改进的NAT——NAPT。一般把在计算机端口上做NAT的技术称为网络地址端口转换（NAPT）技术。

在Windows下可以用软件Sygate Office Network进行NAT配置。SyGate是一套允许使用者在局域网中，通过一个国际互联网连接，分享给整个局域网的使用者，让两台以上的电脑同时上网的好软件，支持Modem/ISDN/Cable Modem只需要在局域网中有Modem的电脑上安装即可，让家中两台以上的电脑都能上网。使用序列号为：H1001001。

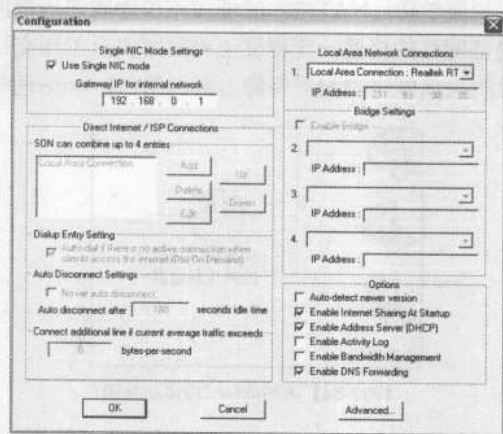
通常，作为NAT服务器的网关，应该拥有多个物理网络接口（即网卡）。如果本机是一台普通电脑，一般只安装了一块网卡，但同样可以使用Sygate Office Network来配置和启用NAT服务。这样一块物理网卡就变为了两块逻辑网卡。Sygate Office Network的操作比较简单，具体步骤如下：

- (1) 安装后，打开运行的主界面，如图2-35所示。单击主界面上的“Configuration”按钮。



【图2-35】Sygate Office Network的主界面

(2) 在弹出“Configuration”对话框中，默认配置要求内网机器的IP地址设在192.168.0.0/24的网络中，并且将网关设为192.168.0.1，如图2-36所示。这样，内部网络的机器便可以通过Sygate Office Network的代理上网了。



【图2-36】 Sygate Office Network的Configuration对话框

2.4 端口基础知识介绍

说到服务，首先要明白“连接”和“无连接”的概念。最简单的例子莫过于打电话和写信。两个人如果要通电话，得首先建立连接——即拨号，等待应答后才能相互传递信息，最后还要释放连接——即挂电话。写信就没有那么复杂了，地址姓名填好以后直接往邮筒一扔，收信人就能收到。

因特网上最流行的协议是TCP/IP协议，需要说明的是，TCP/IP协议在网络层是无连接的（数据包只管往网上发，如何传输和到达以及是否到达由网络设备来管理）。而一旦谈“端口”，就已经到了传输层。协议里面低于1024的端口都有确切的定义，它们对应着因特网上常见的一些服务。这些常见的服务可以划分为使用TCP端口（面向连接如打电话）和使用UDP端口（无连接如写信）两种。

2.4.1 端口的含义

PORT，意思为港口，但在电脑里叫端口。但是端口不是形象的，而是抽象的。电脑上有很多的端口（65535个），但是它们大部分都不开，每个网络连接都要用一个端口。就像把用一根线把两个电脑连起来，插座就是端口。有些端口有他们特定的用途，例如网页服务器要开80端口；FTP服务器要开21端口。

端口（Port）分为物理意义上的端口和逻辑意义上的端口。物理意义上的端口是指在安装在网络硬件设备（ADSL Modem、集线器、交换机、路由器等）上用于连接其他网络设备的接口，如RS-232接口、RJ-45接口、RJ-11接口、SC接口等等。逻辑意义上的端口一般指TCP/IP

协议中的端口，端口对应着上层服务，端口以端口号来表示。端口号的范围从0到65535，比如www服务器使用的是80端口，FTP服务器使用的是21端口。本书中的端口若没有特别说明，均指TCP/IP协议中的端口。

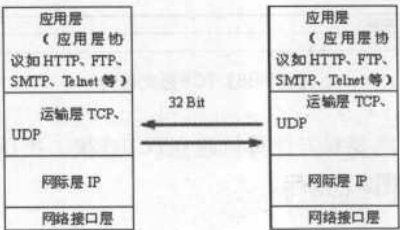
在上一章中我们谈到netstat命令的时候，已经接触了一些关于端口的知识。本节我们就端口的定位、打开、关闭、监控和扫描进行详细讨论。

2.4.2 TCP/IP协议

谈到端口就不得不介绍TCP/IP协议，这里了解一下计算机是如何进行通信的。

首先简要介绍Internet的基本通信协议TCP/IP协议。

TCP/IP，即传输控制协议／网际互连协议，它把整个计算机通信网划分为应用层、运输层、网际层、网络接口层。按照这种层次划分的通信模式如图2-37所示。



【图2-37】TCP/IP通信模式

Internet的网络通信大多是建立在这个协议之上的，各个主机遵循着TCP/IP协议封装数据包进行通信。

由图2-37可见，TCP/IP在运输层包括两个协议TCP和UDP，并且TCP和UDP都使用相同的网际层IP，TCP与UDP协议各自特点如下：

① 用户数据报协议UDP（User Datagram Protocol）：UDP在传送数据之前不需要先建立连接。远地主机的运输层在收到UDP数据报后，不需要给出任何确认。广泛应用于只需一次的客户／服务器模式的请求-应答查询，或者要求提供高效率数据传输的场合。

② 传输控制协议TCP（Transmission Control Protocol）：TCP提供可靠的、面向连接的运输服务，用于高可靠性数据的传输。TCP具有完善的错误检测与恢复、顺序控制和流量控制等功能。

TCP和UDP协议说明如下。

注重可靠性的场合一般使用TCP协议，例如FTP、Telnet，而在那些更注重实时性、传输率、吞吐量的场合一般使用UDP，如QQ。TCP报文分为首部和数据两部分。TCP报文段首部的前20个字节是固定的，后面有4n字节（n为整数）是可有可无的选项。因此TCP首部的最小长度是20字节。TCP报文结构如图2-54所示。

SYN：该标志位用来建立连接，让连接双方同步序列号。如果SYN=1而ACK=0，则表示该数据包为连接请求，如果SYN=1而ACK=1则表示接受连接。

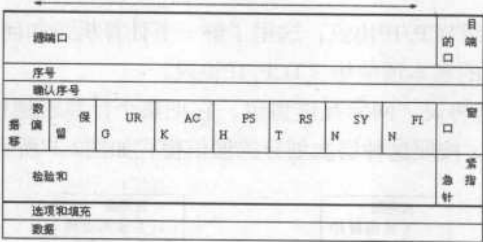
FIN：表示发送端已经没有数据要求传输了，希望释放连接。

RST：用来复位一个连接。RST标志置位的数据包称为复位包。一般情况下，如果TCP收到的一个分段明显不是属于该主机上的任何一个连接，则向远端发送一个复位包。

URG：为紧急数据标志。如果它为1，表示本数据包中包含紧急数据。此时紧急数据指针有效。

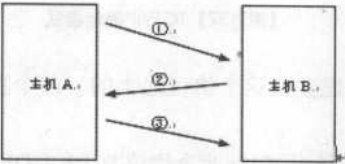
ACK：为确认标志位。如果为1，表示包中的确认号时有效的。否则，包中的确认号无效。

PSH：如果置位，接收端应尽快把数据传送给应用层。



【图2-38】TCP报文结构

当使用TCP协议的时候，需要双方计算机建立TCP连接，把这个建立过程形象地称为“三次握手”。三次握手的过程如图2-39所示。



【图2-39】三次握手的过程

第一次：主机A的TCP向主机B的TCP发出连接请求报文段，首部中的同步比特SYN=1，ACK=0，同时选择一个序号x，表明在后面传送数据时的第一个数据字节的序号是x。

第二次：主机B的TCP收到连接请求报文段后，如同意，则发回确认。在确认报文段中应将SYN=1，ACK=1，确认序号应为x+1，同时也为自己选择一个序号y。

第三次：主机A的TCP收到此报文段后，还要向B给出确认ACK=1，确认序号为y+1。

三次握手后，主机A和主机B就可以相互进行数据传输。

三次握手的功能：保证双方都相互知道对方已准备好进行数据传输，双方确认一个数据传输的初始序列号。例如，发送方的初始序列号为x，接收方初始序列号为y，均被对方确认。

此外，这里简单介绍一下最近比较流行的IPv6协议。IPv6协议全称Internet Protocol Version 6，即IP协议的6.0版本，通常又称为下一代因特网协议，IPv6是Internet工程任务组（IETF）开发设计的用来替代现行IPv4协议的一种新IP协议。IPv6和IPv4作用大致相同，开发的目的是为了缓解IPv4地址空间的压力，另外还弥补了IPv4协议的一些问题，包括端对端IP连接、服

务质量（QoS）、安全性、扩展性及即插即用等。

TCP/IP协议的端口用端口号来表示。从简单意义上理解，一个端口对应一种上层服务。比如端口80就对应着HTTP协议的服务（www网页服务）。由于计算机可以提供的服务很多，而且新服务还在不断出现，所以用两个字节（16bit）来表示端口。16bit的二进制数供有65536种不同的组合，因此端口号的范围从0开始，最大到65535。这些端口划分为两类：

①知名端口（Well-Known Ports）

知名端口上对应的服务是众所周知的，范围从0到1023，这些端口号一般固定分配给某些特定服务。比如21端口分配给FTP服务，23端口分配给TELNET服务，25端口分配给SMTP（简单邮件传输协议）服务，80端口分配给HTTP服务，135端口分配给RPC（远程过程调用）服务等。

②动态端口（Dynamic Ports）

动态端口的范围从1024到65535，这些端口号一般不固定分配给某个服务，也就是说许多服务都可以使用这些端口。只要程序向系统提出访问网络的申请，那么系统就从众多动态端口中自动随机分配一个空闲的端口供该程序使用。比如QQ登录服务器后，向操作系统提出端口申请，操作系统发现端口4000目前是“空闲”的，就将4000端口分配给QQ程序，并将4000端口标记为“占用”。若其他程序需要申请4000端口时，不会再将此“占用”的端口分配出去。当关闭QQ程序进程后，操作系统释放4000端口，并将4000端口的状态重新标记为“空闲”。

将端口划分为知名端口和动态端口两类和上层协议的标准化紧密相关。如果上层协议已经作为标准协议出现，那么就必须为该协议分配一个端口，使得使用该协议的客户端能够自动连接到这个固定分配的端口接受服务，而不再由人来协商。如果上层协议还没有作为标准，则只能在动态端口的范围内动态监听，监听的端口必须通过人为方式告知客户。

2.4.3端口扫描的概念及分类

端口扫描是指利用Socket编程与目标主机的某些端口建立TCP连接、进行传输协议的验证等，从而使知目标主机的扫描端口是否是处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等等。常用的扫描方式有：Connect扫描、Fragmentation扫描。

黑客在攻击之前，扫描一个系统是绝对不可缺的。黑客攻击就和战争一样，知己知彼，方能百战不殆。如果一个黑客连自己将要攻击站点的系统都不知道，真不知道他还能干什么。

2.4.4 常见端口扫描技术

常见的端口扫描技术有三种，下面简要介绍这三种扫描技术：

1.TCP connect扫描

TCP connect扫描（又称为全TCP连接扫描）是最基本的TCP扫描方式。全TCP连接是长期以来TCP端口扫描的基础。扫描主机尝试（使用三次握手）与目的机指定端口建立正规的连

接。连接由系统调用connect开始。对于每一个监听端口，connect会获得成功，否则返回-1，表示端口不可访问。由于通常情况下，这不需要什么特权，所以几乎所有的用户（包括多用户环境下）都可以通过connect来实现这个技术。

这种扫描方法很容易检测出来（在日志文件中会有大量密集的连接和错误记录）。Courtney, Gabriel和TCP Wrapper监测程序通常用来进行监测。另外，TCP Wrapper可以对连接请求进行控制，所以它可以用来阻止来自不明主机的全连接扫描。

2.TCP SYN扫描

TCP SYN扫描（也称为TCP 半连接扫描）。

在这种技术中，扫描主机向目标主机的选择端口发送SYN数据段。如果应答是RST，那么说明端口是关闭的，按照设定就探测其它端口；如果应答中包含SYN和ACK，说明目标端口处于监听状态。由于所有的扫描主机都需要知道这个信息，传送一个RST给目标机从而停止建立连接。由于在SYN扫描时，全连接尚未建立，所以这种技术通常被称为半打开扫描。SYN扫描的优点在于即使日志中对扫描有所记录，但是尝试进行连接的记录也要比全扫描少得多。缺点是在大部分操作系统下，发送主机需要构造适用于这种扫描的IP包，通常情况下，构造SYN数据包需要超级用户或者授权用户访问专门的系统调用。

3.秘密扫描

秘密扫描技术使用FIN数据包来探测端口。当一个FIN数据包到达一个关闭的端口，数据包会被丢掉，并且会返回一个RST数据包。否则，当一个FIN数据包到达一个打开的端口，数据包只是简单的丢掉（不返回RST）。

由于这种技术不包含标准的TCP三次握手协议的任何部分，所以无法被记录下来，从而必SYN扫描隐蔽得多。另外，FIN数据包能够通过只监测SYN包的包过滤器。

还有两种其他的扫描手段值得注意。一种叫做圣诞树扫描，因为它将所有的标记位都置位（不仅仅是SYN, ACK, FIN）；另一种叫做空扫描，因为所有的标记位都被复位。这些秘密的扫描行为将会根据接收端所运行的平台不同而产生不同的错误响应信息。

2.4.5重要的常用端口介绍

电脑在Internet上相互通信需要使用TCP/IP协议，根据TCP/IP协议规定，电脑有256×256（65536）个端口，这些端口可分为TCP端口和UDP端口两种。如果按照端口号划分，它们又可以分为以下两大类：

1.系统保留端口（从0到1023）

这些端口不允许你使用，它们都有确切的定义，对应着因特网上常见的一些服务，每一个打开的此类端口，都代表一个系统服务，例如80端口就代表Web服务。21对应着FTP，25对

应着SMTP、110对应着POP3等，如下所示。

部分常用的知名端口和端口对应的上层服务

端口	对应服务名	对应服务英文全称	对应服务中文名
20	ftp-data	File Transfer[Default Data]	文件传输协议（默认数据口）
21	ftp	File Transfer[Control]	文件传输协议（控制）
22	ssh	SSH Remote Login Protocol	SSH远程登录协议
23	telnet	Telnet	终端仿真协议
25	smtp	Simple Mail Transfer	简单邮件发送协议
53	domain	Domain Name Server	域名服务器
64	covia	Communications Integrator (CI)	通讯接口
65	tacacs-ds	TACACS-Database Service	TACACS数据库服务
66	sql*net	Oracle SQL*NET	Oracle SQL*NET
67	bootps	Bootstrap Protocol Server	引导程序协议服务端
68	bootpc	Bootstrap Protocol Client	引导程序协议客户端
69	tftp	Trivial File Transfer	小型文件传输协议
79	finger	Finger	查询远程主机在线用户等信息
80	http	World Wide Web HTTP	全球信息网超文本传输协议
92	npp	Network Printing Protocol	网络打印协议
93	dcp	Device Control Protocol	设备控制协议
109	pop2	Post Office Protocol - Version 2	POP2电子邮局协议版本2
110	pop3	Post Office Protocol - Version 3	POP3电子邮局协议版本3
111	RPC	Remote Procedure Call	远程过程调用
135	Location Service	Location Service	Windows的RPC服务端口
137	NETBIOS Name Service	NETBIOS Name Service	NETBIOS名字服务
138	NETBIOS Datagram Service	NETBIOS Datagram Service	NETBIOS数据报
139	NETBIOS Session Service	NETBIOS Session Service	NETBIOS会话
143	IMAP2	Interim Mail Access Protocol v2	IMAP邮件访问协议
156	SQL Service	SQL Service	标准SQL服务
443	https	Secure HTTP	安全HTTP服务
444	SNPP	Simple Network Paging Protocol	SNPP协议
445	Microsoft-DS	Microsoft-DS	微软目录服务
554	RTSP	Real Time Streaming Protocol	实时流协议RTSP



端口也可以分为TCP端口和UDP端口。在TCP端口监听的上层软件利用传输层提供的TCP服务进行传输。在UDP端口监听的上层软件利用传输层提供的UDP服务进行传输。

2.动态端口（从1024到65535）

当你需要与别人通信时，Windows会从1024起，在本机上分配一个动态端口，如果1024端口未关闭，再需要端口时就会分配1025端口供你使用，依此类推。

但是有个别的系统服务会绑定在1024到49151的端口上，例如3389端口（远程终端服务）。从49152到65535这一段端口，通常没有捆绑系统服务，允许Windows动态分配给你使用。

3.获取最新端口分配信息

IANA是分配知名端口的官方组织。可以访问IANA的主页获得最新的端口分配信息：<http://www.iana.org/assignments/port-numbers>，如图2-40所示。



【图2-40】最新的端口分配信息

2.5 小结

本章介绍了IP地址和端口的一些基本知识。通过介绍，可以了解到入侵者如何通过搜索引擎、扫描器来探知目标主机、服务器的敏感信息。其中强大的综合扫描器是入侵者必不可少的工具。作为防御端，如何更有效减少关键信息的泄露便成为了安全防御的第一步。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第3章 聊天黑客工具

在网络的使用中，聊天占了一席之地，用于娱乐的聊天、视频，用于工作交流的工作组等等。实时聊天工具也有很多，本章将为读者介绍一些必备的基础知识。

本章要点

- ◎ QQ盗号与防范
- ◎ QQ破坏防范
- ◎ QQ聊天记录窥探与保护

3.1 QQ盗号工具

随着QQ推出各种各样的收费服务以后，花钱去充值QQ币的人越来越多了。当然这其中也少不了想不劳而获，直接盗用他人QQ号的人。

3.1.1 QQ简单盗

QQ简单盗的使用很简单，就是生成木马后发送给其他人，中木马与接收木马的这个QQ号码和密码就会发送到指定的邮箱了。

QQ简单盗有如下特点：

(1) 利用现在比较领先的进程插入技术，使QQ盗本身无进程，无注册码启动项，增加文件自动保护和COM+钩子保护等功能，使程序做到难以查杀和删除。

(2) 使用API-HOOK完美破解QQ2005-QQ2006b1的驱动键盘保护，保证绝对不会出现红叉，包括一些特殊版本，例如珊瑚虫版和飘云版，黑客版、防盗版之类的改版QQ。

(3) 强大的密码截取功能，保证完美地截取密码数据和QQ号码，保证截取QQ目前的所有版本的密码。基本上杜绝了漏记和无法截取的问题。

(4) 提供两种收信功能。

①为了避免丢失邮件等事情的发生，增加了传统的smtp收信。你可以设置自己的发信邮箱和收信邮箱。

②ASP收信。可以通过ASP地址直接将数据更新到你的网站上。

(5) 自选图标功能。可以设置自己生成的木马程序的图标修复原Delphi程序本身的错误代码。(修改的程序图标会变色的问题)许多木马和合并器都有这个错误。使之只能选取已有的*.ico文件，这新版图标为QQ盗号增加了自选图标功能，只要是你看的到的文件图标都可以自动提取出来。程序图标保持原有样式100%不会变色。

(6) 附加功能

①过滤重复号码。只有当用户名和密码与上次登录都不相同的时候才会发信，完全杜绝了重复号码的现象。网站收信方式：上传QQPass.asp即可，默认记录到同路径的QQPass.txt，也可自行修改。

②支持smtp邮箱发信。

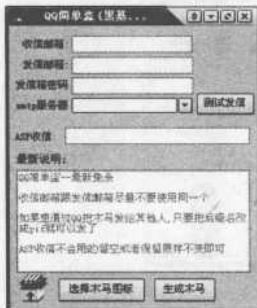
【案例3-1】使用QQ简单盗发送木马盗取QQ号码。

(1) 运行QQ简单盗，弹出主界面，如图3-1所示。在主界面的空白文本框中按照填入收信邮箱和ASP收信的地址等信息，ASP收信是将ASP文件上传至网站，凡是浏览的用户QQ密码都将成为囊中之物。其中smtp服务器栏填入收信邮箱的smtp服务器，例如“smtp.21cn.com”，然后单击“选择木马图标”按钮。

(2) 在弹出的“打开”对话框中选择作为木马图标的图片，以方便隐蔽木马，选择好之后单击“打开”按钮，如图3-2所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 3 章 聊天黑客工具



【图3-1】QQ简单盗主界面



【图3-2】选择作为木马图标图片

- (3) 单击主界面中的“生成木马”按钮，弹出“另存为”对话框，在此对话框中选择保存木马的位置和名称，设置好之后单击“保存”按钮保存木马，如图3-3所示。
- (4) 弹出“提示”对话框，说明木马的名称和保存地址，单击“确定”按钮，如图3-4所示。



【图3-3】保存木马



【图3-4】“提示”对话框

- (5) 刚才将此木马保存到了桌面，在桌面生成了一个叫“服务端”的图片，其实它是一个.exe类型的文件伪装成了一个.jpg图片文件，如图3-5所示。
- (6) 现在打开QQ，给想要盗取的号码发送生成的木马文件，等待对方接收，如图3-6所示。如果对方接收并运行了此木马，那么就可以打开在主界面中输入的接收邮件的邮箱查看收到的包含此QQ号码和密码的邮件了。



【图3-5】生成了木马

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图3-6】发送木马

3.1.2 QQ流感大盗

QQ流感大盗是目前最新版的盗QQ工具，也是技术最全面的一个工具。它能够破解目前最新QQ键盘保护（Beta3版本）。

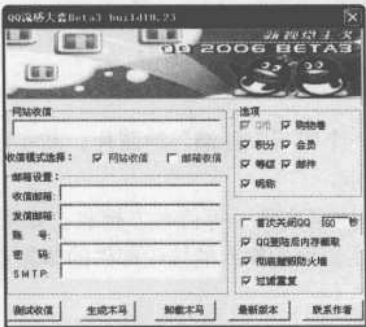
QQ流感大盗有如下特点：

- (1) 密码框不会出现红叉，木马无进程，无启动项。
- (2) 可以截取QQ用户QB、购物卷等信息。
- (3) 准确截取目前的QQ最新版本（Beta3版本）包括以前所有版本。
- (4) 具有收、发信快的特点，而且准确无误。

【案例3-2】使用QQ流感大盗发送木马盗取QQ号码。

(1) 运行QQ流感大盗，弹出主界面，同QQ简单盗一样，设置好收信的网站或者邮箱，不同的是QQ流感大盗还增加了选择要盗取的目标，例如积分、会员、邮件等，如3-7所示。

(2) 单击“生成木马”按钮，弹出“另存为”对话框，选择保存木马的位置，然后单击“保存”按钮，如图3-8所示。



【图3-7】QQ流感大盗主界



【图3-8】生成木马

(3) 弹出“流感”对话框，说明木马已经生成，并且显示保存的位置，如图3-9所示。QQ流感大盗不支持将木马另存为其他格式，直接发送.exe的文件很容易被QQ安全中心拦截，所以可以将木马压缩然后诱使对方解压并运行。

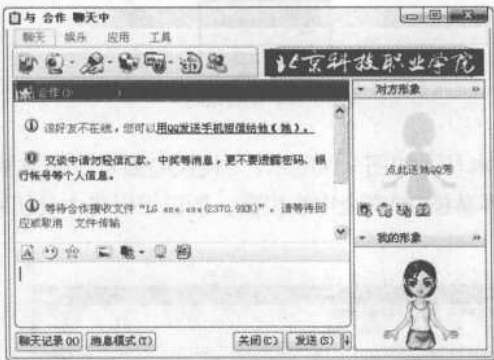
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



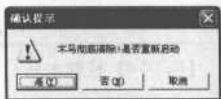
【图3-9】生成木马

(4) 打开QQ，给想要盗取的号码发送生成的木马文件，等待对方接收，如图3-10所示。如果对方接收并运行了此木马，那么就可以打开在主界面，输入接收盗取号码的邮箱地址，然后就能查看包含此QQ号码和密码的邮件了。

(5) QQ流感大盗有个优点就是自带了清除木马功能，因为攻击别人而生成的木马其实自己也保存了，单击QQ流感大盗主界面中的“卸载木马”按钮，弹出“确认提示”对话框，显示木马已经彻底清除，当然这里的木马特指QQ流感大盗生成的木马，是否立即重新启动就按照需要来选择了，也可以单击“取消”按钮推退出，如图3-11所示。



【图3-10】发送木马



【图3-11】清除木马

3.1.3 剑盟QQ盗号王

剑盟QQ盗号王是目前比较“专业”的QQ盗号工具，它的盗号成功率比较大。

【案例3-3】使用剑盟QQ盗号王发送木马盗取QQ号码

(1) 运行剑盟QQ盗号王，弹出主界面，如图3-12所示。在主界面的空白文本框中按照填入收信邮箱和ASP收信的地址等信息，其中smtp服务器栏填入收信邮箱的smtp服务器，由于此软件只支持21.cn邮箱，所以已经默认在邮件服务器栏填入“smtp.21cn.com”，保存路径也是默认在运行剑盟QQ盗号王所在的文件夹，单击“生成”按钮。

3.1.4 QQ防盗及密码取回

随着QQ红遍大地，它受到的黑暗攻势也越来越猛烈，有的恶意用户专门针对QQ编写了流行性病毒、木马等，使网络中的净土腾起了一片尘埃。

毫无疑问，网络即时通讯工具已经成了我们工作、生活中不可缺少的一部分，上网第一步的习惯性操作就是打开QQ、MSN等。一些人甚至把它们的重要性提到了与手机对等的地位，一旦发生QQ密码被盗无法登录的情况损失可谓损失大矣。多年来联系的同学、朋友一去不复返了。正因为如此，大部分人都有防止密码被盗的安全意识，但现在的木马层出不穷，除了平时养成定期修改密码并保证密码的复杂性等良好的习惯外，还应该用软件的专业功能来保护密码，以确保这类软件密码的安全。

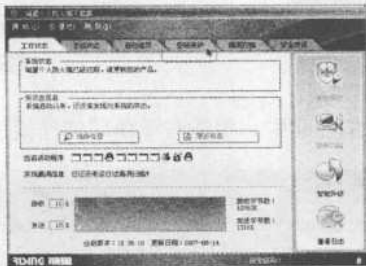
1.使用瑞星防火墙2007版密码保护功能

【案例3-4】使用瑞星防火墙2007版防止QQ被盗。

瑞星防火墙2007版有一个非常强大的功能——“密码保护”功能，可自动识别程序并进行安全防护。通过使用进程墙的技术来实现密码保护功能，可以有效地防止密码盗取和传输。瑞星个人防火墙内置了多款密码的保护功能，用户也可以自己添加受保护的程序。

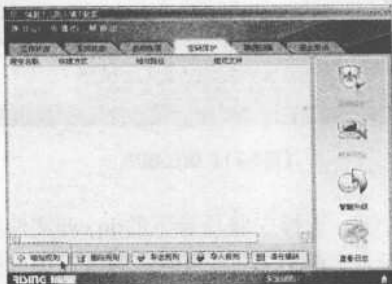
使用瑞星个人防火墙的“密码保护”功能保护QQ密码的安全操作步骤如下：

- (1) 安装瑞星防火墙，打开程序，单击瑞星个人防火墙“密码保护”标签，如图3-16所示。

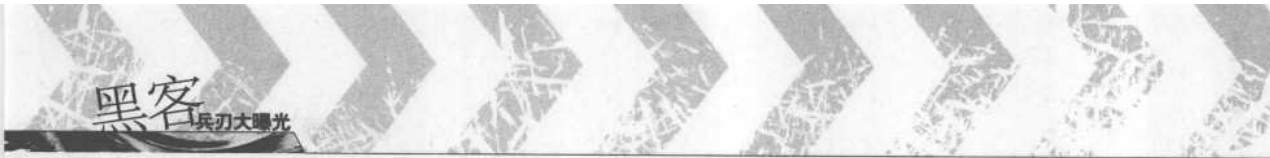


【图3-16】瑞星防火墙主界面

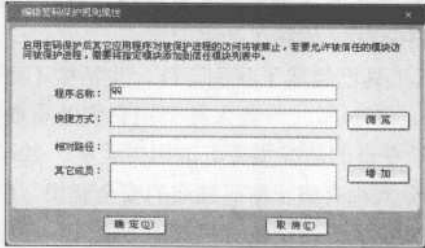
- (2) 单击左下角的“增加规则”按钮，如图3-17所示。



【图3-17】增加规则

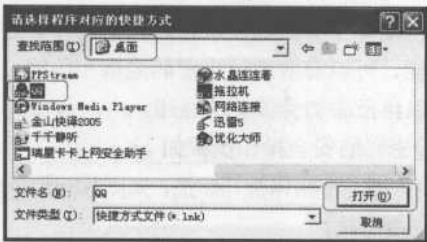


(3) 在“编辑密码保护规则属性”对话框的“程序名称”一栏输入规则名称，例如：“QQ”。然后单击“浏览”按钮，如图3-18所示。

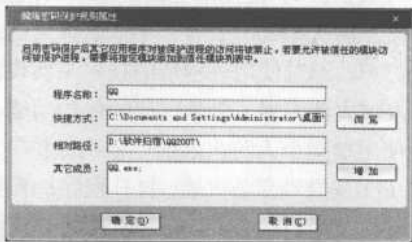


【图3-18】规则名和快捷方式

(4) 选择桌面上的“QQ”图标，程序自动把快捷方式，相对路径等信息提取并添加到规则编辑窗口。单击“确定”按钮完成规则添加，如图3-19所示。添加完毕后自动弹出“编辑密码保护规则属性”对话框，如图3-20所示。

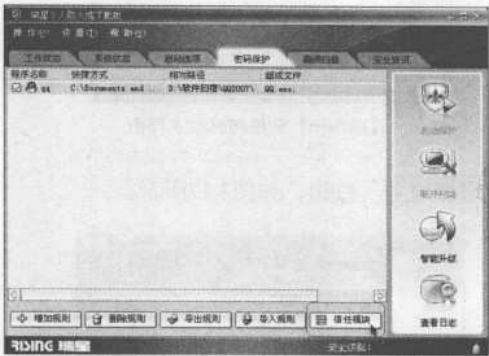


【图3-19】选择桌面上的“QQ”图标



【图3-20】添加成功

(5) 刚才添加的QQ出现在主界面中，单击右下角“信任模块”按钮，如图3-21所示。



【图3-21】信任模块

(6) 单击“增加模块”按钮，选择安装目录下的qq.exe文件加入到信任模块当中，然后单击“打开”按钮，如图3-22所示。QQ出现在受信任的可以访问受密码保护的进程模块列表中，如图3-23所示。至此保护密码的步骤已完成，双击运行QQ程序，瑞星个人防火墙会从桌

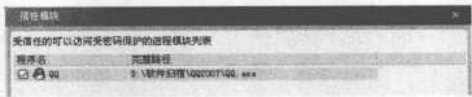
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

面右下角升起泡泡提示防火墙进入“密码保护模式”。此时，程序已经受到保护，可以放心地使用QQ聊天程序，不必再担心密码被盗。

注意：如果将Tm加入密码保护，需要同时将安装目录下的TMDLLS子目录中的TM.exe程序加入到信任模块当中。



【图3-22】增加模块



【图3-23】添加完成

2.使用QQ申诉取回被盗的QQ

所谓百密一疏，在强大保护措施下的QQ也可能由于各种原因被盗。如果QQ已经被盗，并且没有设置第二代密码保护，也不用焦急，还有一招可以取回QQ，那就是QQ申诉。

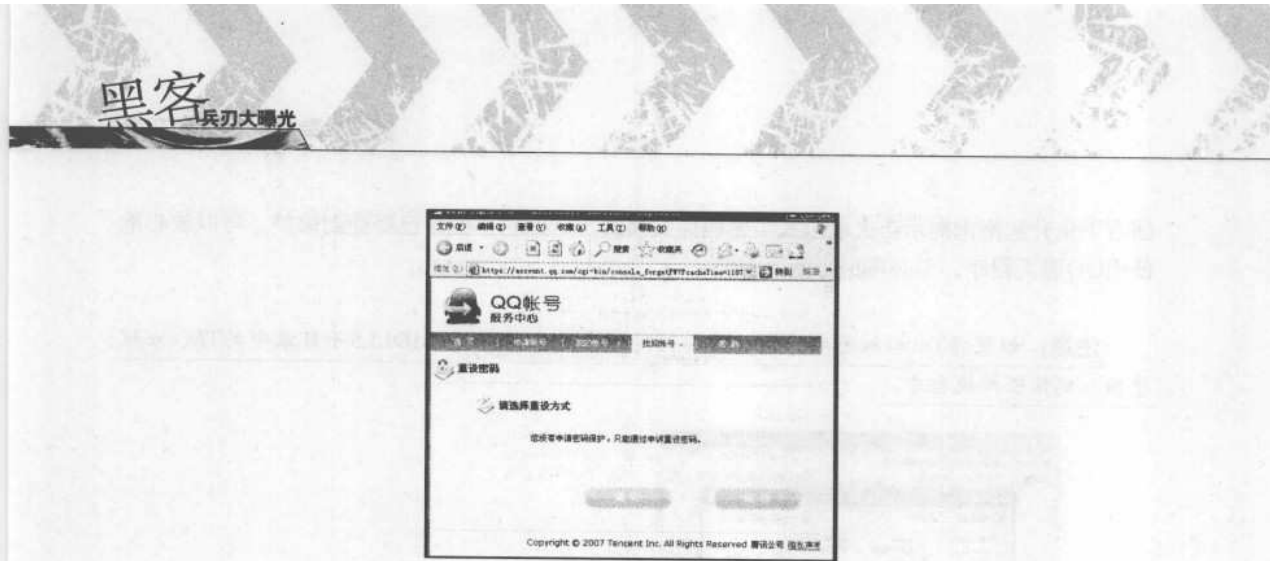
QQ申诉是腾讯提供的一个专门用于忘记密码或者被盗的时候使用的工具，只要能够证明申诉的号码确实为你所有，就可能通过重设密码来取回这个号码。

【案例3-5】使用QQ申诉取回被盗的QQ

- (1) 打开<https://account.qq.com>，单击“找回帐号”，在弹出的“自助重设密码”页面中按照说明填入要求申诉的QQ账号、密码类型和验证码，然后单击“确定”按钮，如图3-24所示。
- (2) 由于没有申请密码保护，要通过申诉来取回密码，单击“确定”按钮，如图3-25所示。

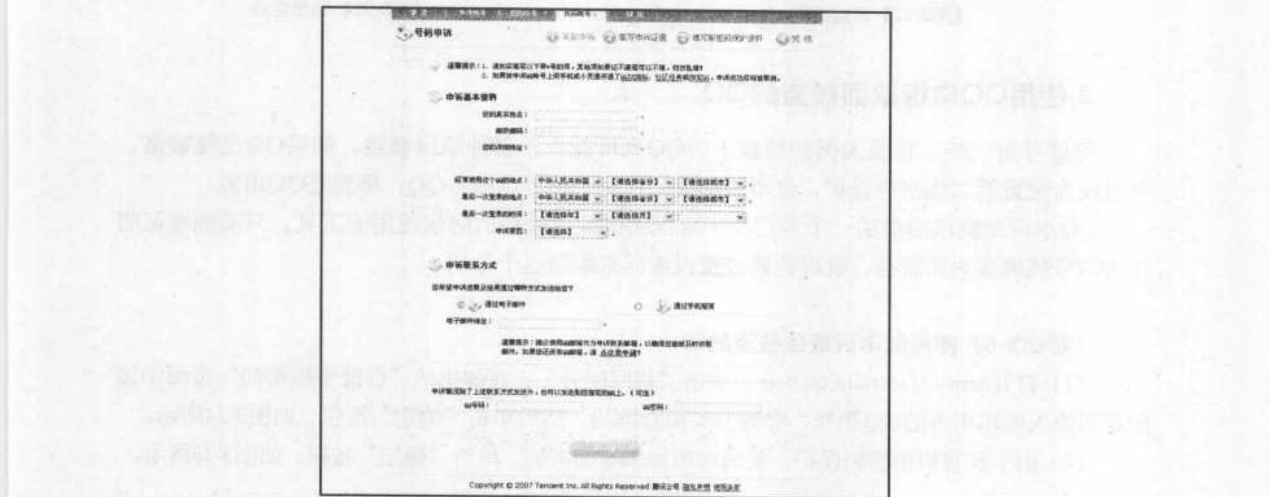


【图3-24】“自助重设密码”页面



【图3-25】选择申诉

(3) 在“号码申诉”页面填入各类信息，带红色星号的为必选项，当然其他项也是越详细越好，因为这样能提供更多的证据。填完之后单击“下一步”按钮，如图3-26所示。



【图3-26】填写申诉说明

(4) 申诉被接受，而且腾讯将申诉回执发送到上一步填的邮箱中，打开邮箱，如图3-27所示。将申诉回执中的验证码填入如图3-28所示的“你收到的验证码”文本框中，再将页面中其他必选项填写完整，然后单击“下一步”按钮。



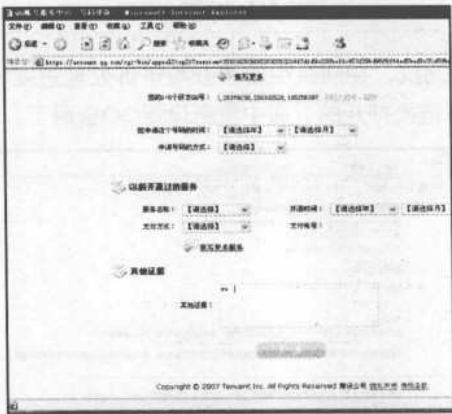
【图3-27】申诉验证码回执

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图3-28】填入验证码等信息

(5) 接下来的页面要求填入QQ好友、申请时间等信息，是为了证明此QQ是属于你的，填得越详细越好，填写好之后单击“下一步”按钮，如图3-29所示。



【图3-29】填入QQ好友、申请时间等信息

(6) 接下来的页面要求填入新的密码保护资料，也就是说如果申诉成功取回了号码，那么此号码就有密码保护了，而且就是现在输入的问题和答案，所以要记住设置的内容，设置好之后单击“下一步”按钮，如图3-30所示。



【图3-30】填入新的密码保护资料

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

黑客
兵刃大曝光

(7) 号码申诉完成，并告知申诉回执编号，而且已经发通知到指定邮箱中，如图3-31所示。



【图3-31】申诉已经受理

(8) 打开邮箱，查收回执，在回执中给了查看申诉处理进度和结果的链接，如图3-32所示。如果申诉成功就可以在链接打开的页面中重新设置QQ密码了，这样就将QQ取回了。



【图3-32】申诉已经受理的邮件

3. 清除QQ木马病毒

清除木马主要有三招：

(1) 手工查杀

由于木马会插入到系统N多线程中如explorer.exe、ctfmon.exe及非系统线程中，这里无须一一寻找（相对于普通网络用户来说难度系统较大），直接从系统中搜索newqq.dll并删除（这里可以用强行删除文件工具进行删除），完成后重启计算机即可。

(2) 使用相关专业软件进行清理

推荐使用QQ病毒专杀工具XP QQ Kav2007版，此版本可以查杀流行的QQ木马病毒及其变种（15000余种），并加强对病毒注册表残留病毒项清理清除功能，对一些垃圾流氓插件也有

一定的清理作用。

(3) 使用木马清除大师2007

此软件具有病毒库实时更新快，针对流行的木马杀力特强，操作简易上手，其九大实时监控有效观察系统里的一举一动，扩充的病毒库可实现对六万多种木马间谍的查杀。

3.1.5 简单反击盗QQ者

简单反击盗QQ者是专门针对盗号木马的一个反击工具，因为盗号者要将盗取的号码和密码发送到自己的邮箱中，而简单反击盗QQ者的原理是利用嗅探，随便用错密码登QQ，嗅探到盗号者的邮箱用户名和密码。

- (1) 打开GUI版X-sniffer，单击“开始监听”。
- (2) 登录QQ，用错密码。
- (3) GUI版x-sniffer文件夹下生成新文件：“pass.log”，里面就是盗号者的邮箱用户名和密码。

【案例3-6】使用简单反击盗QQ者取回被盗的QQ。

使用简单反击盗QQ者具体步骤如下：

- (1) 运行简单反击盗QQ者，弹出主界面，单击“开始监听”按钮，如图3-33所示。

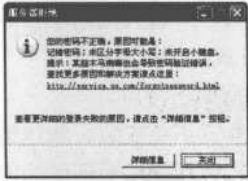


【图3-33】简单反击盗QQ者主界面

- (2) 登录QQ，随便使用一个密码，如图3-34所示。
- (3) QQ已经被盗了，弹出密码错误，服务器拒绝的对话框，如图3-35所示。



【图3-34】登录QQ



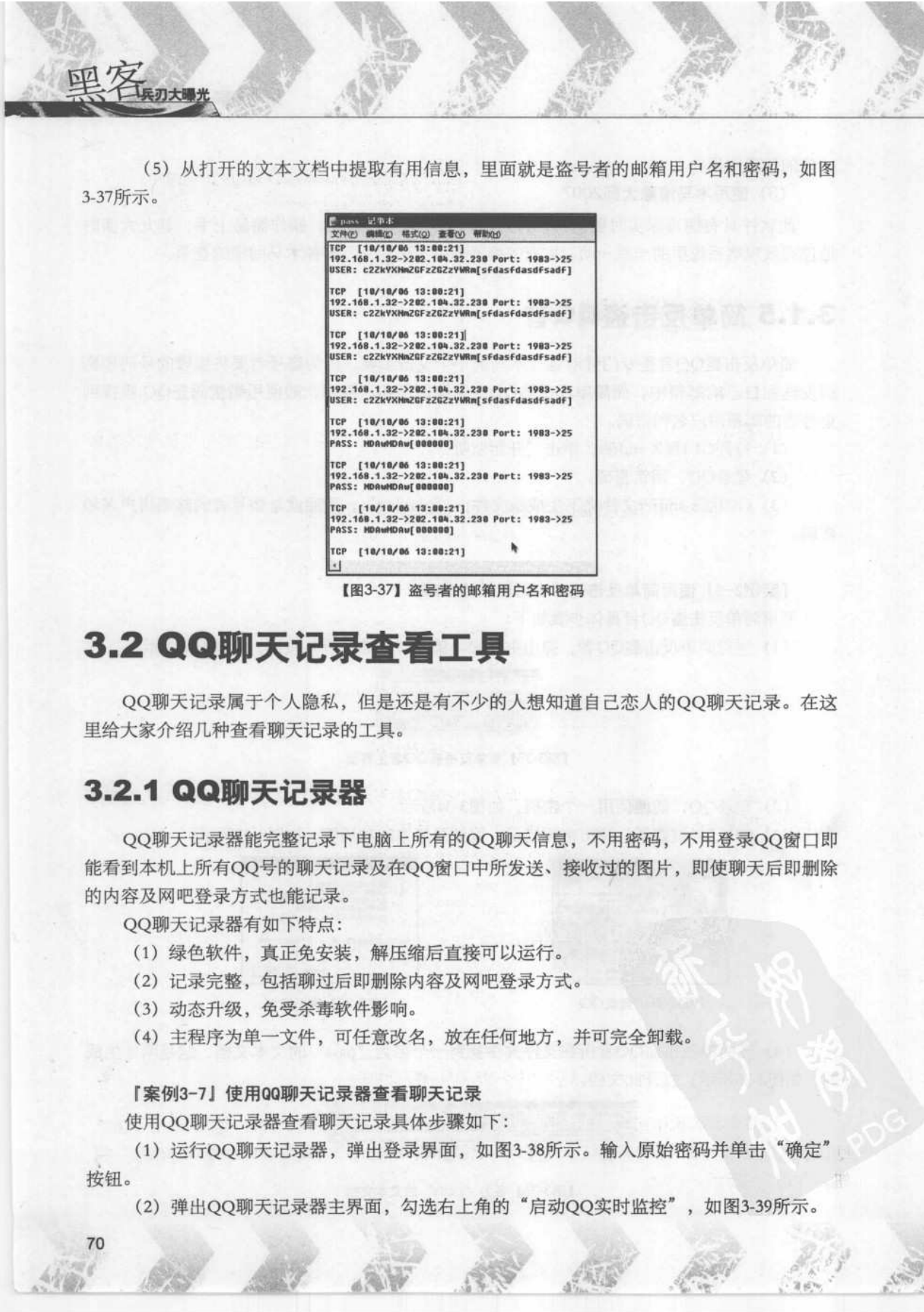
【图3-35】密码错误

- (4) 在简单反击盗QQ者所在文件夹中找到一个名为“pass”的文本文档，这是刚才生成的，如图3-36所示，打开此文档。



【图3-36】名为“pass”的文本文档

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

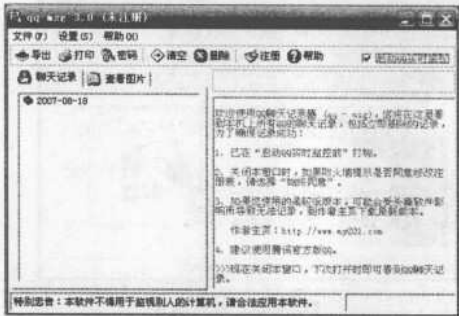


【图3-38】QQ聊天记录器登录界面



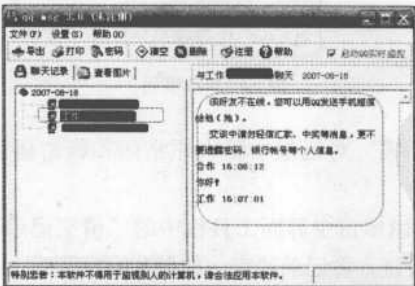
【图3-39】QQ聊天记录器主界面

(3) 登录QQ，在主界面左下方的空白方框中显示了QQ登录的日期，此时默认选定的是查看聊天记录，如图3-40所示。



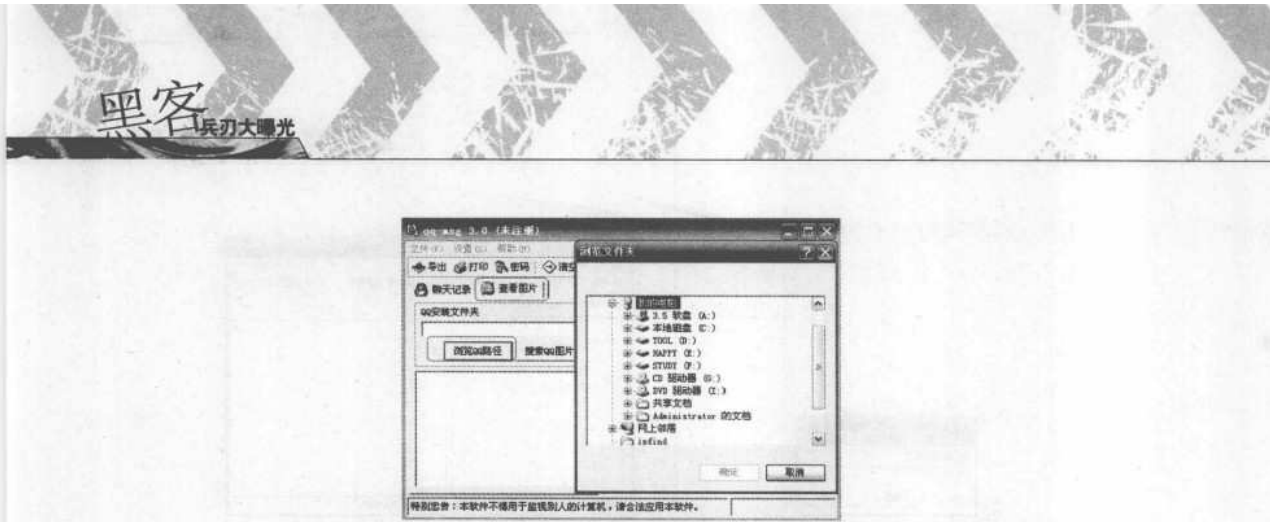
【图3-40】显示QQ登录的日期

(4) 进行QQ聊天，此时，在主界面左侧的方框中显示出了正在聊天的自己和好友的名称和QQ号码，而右侧的方框中则显示聊天的内容，如图3-41所示。



【图3-41】实时记录QQ聊天的内容

(5) 要查看聊天中出现过的图片，单击主界面中的“查看图片”按钮，然后单击“浏览QQ路径”按钮，在弹出的“浏览文件夹”对话框中选择安装QQ的路径，然后单击“确定”按钮，如图3-42所示。



【图3-42】查看图片

(6) 聊天中出现过的图片名称显示在左下角的空白处，单击其中一个名称，则对应的图片就出现在右边，如图3-43所示。



【图3-43】显示图片

(7) 为了防止别人随意使用，可以修改QQ聊天记录器的密码，单击菜单栏的“设置”，在弹出的下拉菜单中单击“修改密码”，如图3-44所示。

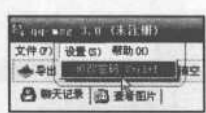
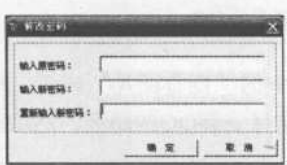


图3-44 修改密码

(8) 在弹出的“修改密码”对话框中输入原密码和新密码后单击“确定”按钮，如图3-45所示。

(9) 如果要清空记录可以单击主界面工具栏中的“清空记录”工具，然后在弹出的“警告”对话框中单击“确定”按钮，将记录清空，如图3-46所示。



【图3-45】“修改密码”对话框



【图3-46】清空记录

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(10) 如果要导出记录另外保存，可以单击主界面工具栏的“导出”工具，然后在弹出的“另存为”对话框中选择要保存的地址，然后单击“保存”按钮就可以了，如图3-47所示。



【图3-47】导出聊天记录

3.2.2 QQ聊天终结者

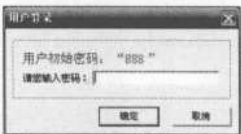
QQ聊天记录终结者2007集成版能完全实时记录（QQ/TM）2007及以下各版本的聊天记录（包括群消息），及图片信息。无论（QQ/TM）用户是否选择保存聊天记录，即使以网吧模式进入，或后来删除的聊天记录，本软件都能完整记录下来。

QQ聊天记录终结者有如下特点：

- (1) 支持所有（QQ/TM）2007及以下版本，完整记录聊天消息及图片信息。
- (2) 无遗漏的记录（QQ/TM）的全部消息、图片，包括（群消息）。
- (3) 支持远程记录（QQ/TM）消息的功能。
- (4) 提供（邮件通知）功能，将记录的消息发送到你指定的邮箱。
- (5) 可以只记录你感兴趣的（QQ/TM）号码的聊天消息。
- (6) 界面美观，操作简单。提供消息查看器方便你查看本地消息。
- (7) 完全绿色版本，不留痕迹。

【案例3-8】使用QQ聊天记录终结者2007集成版。

- (1) 安装QQ聊天记录终结者2007集成版，运行此软件，弹出“用户登录”对话框，输入初始密码，然后单击“确定”按钮，如图3-48所示。
- (2) 弹出QQ聊天记录终结者2007集成版主界面，如图3-49所示。状态栏显示“当前没有监控”，单击工具栏中的“新建监控”。



【图3-48】“用户登录”对话框图



【3-49】QQ聊天记录终结者2007集成版主界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

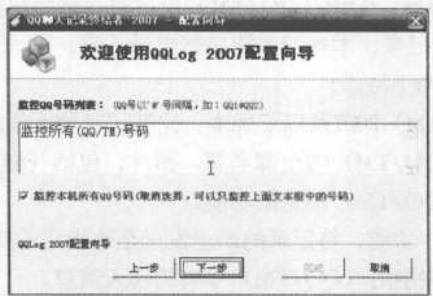


(3) 弹出“配置向导”，选择新建监控的名称和本地数据库路径，然后单击“下一步”如图3-50所示。



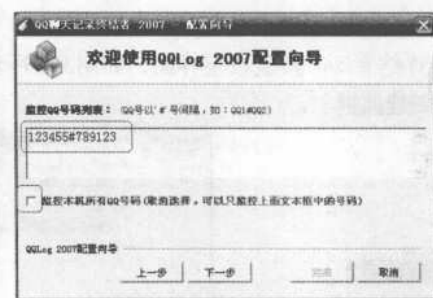
【图3-50】选择新建监控的名称和本地数据库路径

(4) 在弹出的对话框中选择要监控本机所有QQ号码还是有选择地监控，默认为监控所有号码，如图3-51所示。



【图3-51】监控本机所有号码

(5) 如果只想监视特定的号码则取消勾选“监控本机所有QQ号码”，然后在“监控QQ号码列表”栏中输入要监控的号码，两个号码中间用“#”隔开，然后单击“下一步”按钮，如图3-52所示。



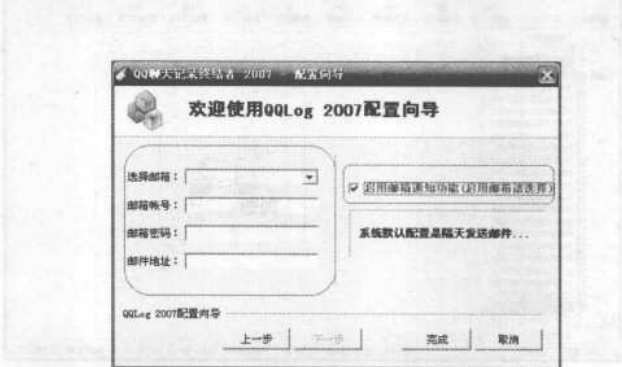
【图3-52】监控指定号码

(6) 此时询问是否启用邮箱通知功能，就是把聊天记录发送到指定的邮箱，如果要发送

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 3 章 聊天黑客工具

就填写邮件地址和密码，然后单击“下一步”按钮；不发送则单击“完成”按钮完成设置，如图3-53所示。



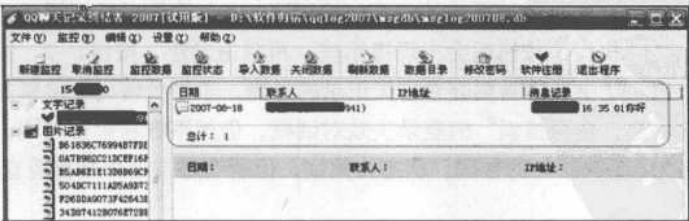
【图3-53】询问是否启用邮箱通知功能

(7) 监控开始运行，如图3-54所示。



【图3-54】监控开始运行

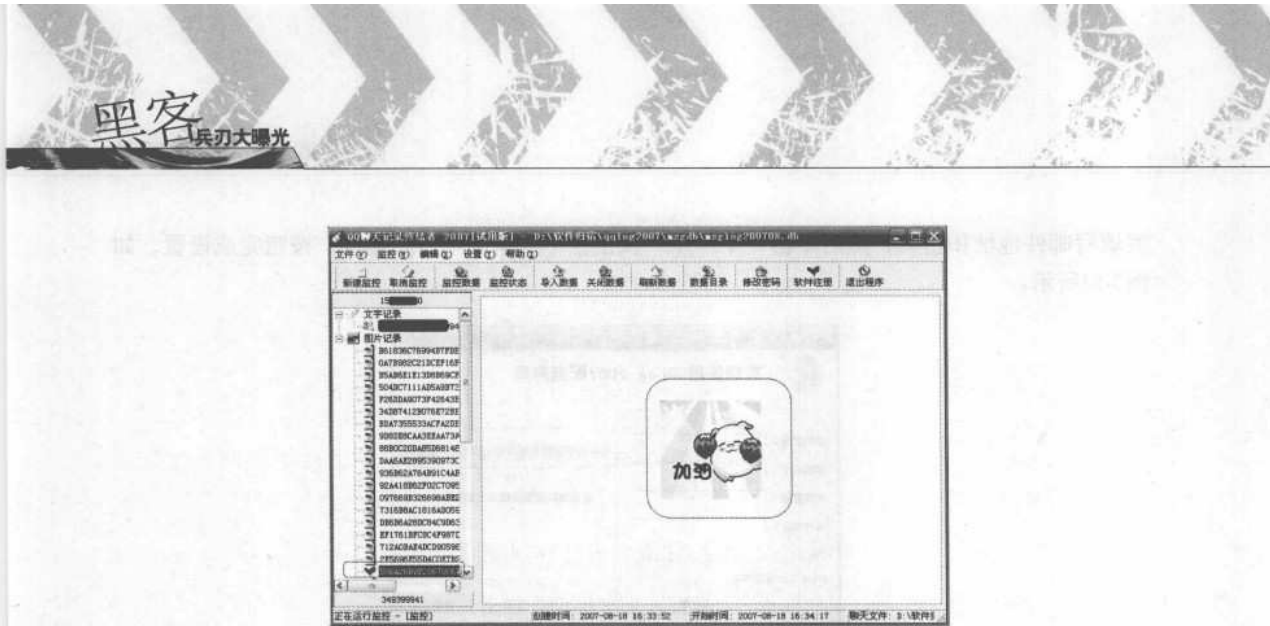
(8) 聊天的文字记录和图片记录都出现在主界面的左侧呈树形目录，而聊天记录则显示在右边以表格的形式显示，如图3-55所示。



【图3-55】显示聊天文字记录

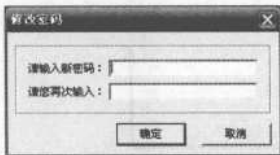
(9) 如果要查看图片则单击树形目录中的某一幅图片，此图片就出现在右侧区域中，如图3-56所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

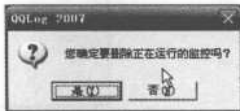


【图3-56】查看图片

- (10) 为了防止别人随意使用，可以修改QQ聊天记录终结者的密码，单击工具栏的“修改密码”工具，在弹出的“修改密码”对话框中输入新的密码然后单击“确定”按钮，如图3-57所示。
- (11) 取消监控可以单击工具栏中的“取消监控”工具，在弹出的对话框中单击“是”按钮即可，如图3-58所示。



【图3-57】修改密码



【图3-58】取消监控

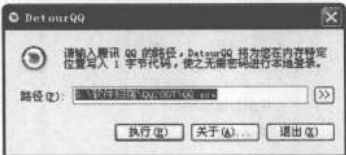
3.2.3 DetourQQ

这款软件使用非常简单，下载解压后只有一个可运行文件“detourqq.exe”和一个说明文件，注意双击可执行文件时关掉系统的病毒监控程序。1、软件对话框提示首先正确定位到本机qq安装目录，单击执行”按钮后会出现提示框，再单击确定”按钮。2、接着就会弹出qq登录窗口，从qq号码一栏中选择需要查看聊天记录的号码，不用管密码直接单击登录按钮。3、紧接着会弹出“对不起，密码错误”的登录失败对话框，仍然不管它单击关闭。此时其实已经登录了本机一个名为12343668”的号码，状态为离线，但所有好友名单却都能查看。

【案例3-9】使用DetourQQ查看聊天记录

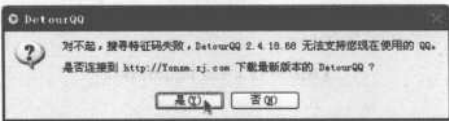
- (1) 运行DetourQQ，在弹出的对话框中自动搜寻到了本机QQ的安装路径，要在内存中写入一字节代码，询问是否执行。单击“执行”，如图3-59所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



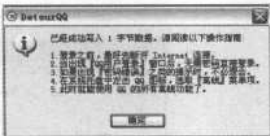
【图3-59】执行写入内存

(2) 由于使用的QQ版本是2007版，DetourQQ目前的版本暂时还不支持QQ2007以上的版本，所以弹出如图3-60所示的失败对话框。



【图3-60】写入失败

(3) 目前的DetourQQ支持QQ2006以及以下的版本，为了演示DetourQQ的使用步骤假设写入成功。如果QQ2006以及以下的版本或者在DetourQQ推出更新的支持QQ2007的版本之后就会弹出如图3-61所示的界面。



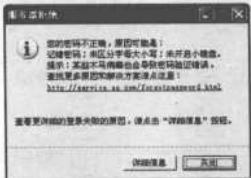
【图3-61】写入成功

(4) 打开QQ登录界面，输入要查看的QQ号码，随便输入一个密码，如图3-62所示。

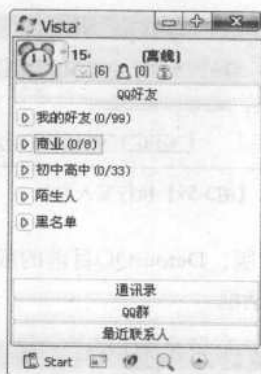


【图3-62】输入账号和密码

- (5) 弹出“服务器拒绝”对话框，如图3-63所示，不用理会。
- (6) QQ界面已经出现了，但是离线状态，可以进行查看好友等操作了，如图3-64所示。



【图3-63】密码错误



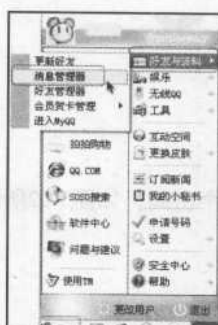
【图3-64】离线状态的QQ

3.2.4 不用软件手工查看QQ聊天记录

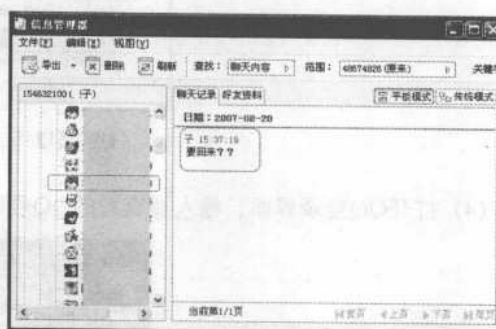
1. 如果想查看本机的QQ聊天记录，登录后可以查看到。

(1) 依次单击“系统菜单”→“好友与资料”→“消息管理器”，如图3-65所示。

(2) 在消息管理器中左边“我的好友”里面选中要查看的好友，右边就会显示出聊天记录，如图3-66所示。



【图3-65】登录QQ后打开“消息管理器”



【图3-66】查看“消息管理器”中的聊天记录

(3) 如果要查看在本机使用过，但不知道登录密码的QQ聊天记录。可以直接从本机中提取。打开资源管理器，打开QQ安装目录下某个QQ号码的文件夹，找到一个名为“Msgdb”的数据库，里面就是此号码的QQ在本机上的全部聊天记录。



【图3-67】“Msgdb”数据库

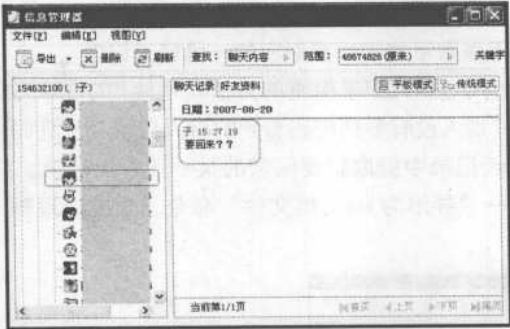
3.2.5 QQ聊天记录保密

与任何一位好友进行QQ聊天的所有记录全部被自动保存在自己QQ号码文件夹中，如果直接将自己QQ号码文件夹删除掉，虽然可以达到驱除聊天记录的目的，不过这么一来保存在QQ号码文件夹中的好友分组内容、QQ表情等内容也将被一并删除，很显然这种删除聊天痕迹的做法会“殃及无辜”。

【案例3-10】只删除聊天记录文件。

有没有办法只删除具体的聊天内容，而不删除好友分组内容、QQ表情等内容呢?答案是肯定的，我们可以按照如下操作步骤，来实现只删除聊天记录文件的目的：

打开Windows系统资源管理器窗口，进入到QQ文件夹窗口，并从中找到对应自己QQ号码的文件夹，鼠标双击该文件夹图标，打开自己QQ号码的文件夹窗口；在该文件夹窗口中，找到一个名为“Msgex.db”的文件，如图3-68所示。然后用鼠标右键单击该文件，从出现的快捷菜单中单击“删除”命令，这样的话保存聊天记录的具体文件就会从计算机系统中消失了，此时重新登录进QQ时，就会发现聊天痕迹找不到了，但是好友分组内容、QQ表情、QQ场景等信息依然存在。



【图3-68】找到要删除的聊天记录

当然，要是只是想阻止其他人偷窥聊天记录的话，没有必要将保存聊天记录的“Msgex.db”文件彻底删除掉，而可以将“Msgex.db”的文件名称修改成其他名称，这样一来重新登录QQ时也会发现聊天痕迹全部被清除干净了，那么其他人就偷窥不到自己的聊天记录了。日后，当自己想查看以前的聊天内容时，只要再将更名之后的目标聊天记录文件重新命名为“Msgex.db”，就可以全部恢复过来了。

虽然通过删除文件的方法，能非常方便、快捷地将所有的聊天痕迹清除干净，但是这种删除方法有点过于“彻底”，要么毫无保留，要么一个不删。那有没有办法只删除“见不得光”的聊天记录，而将其他有用的聊天记录保存下来呢？

要做到这一点，必须从QQ程序的消息管理器着手，对聊天信息进行有针对性的管理，前提是要登录QQ后才能进行操作。下面就是该方法的具体实现步骤：

- (1) 依次单击“系统菜单”→“好友与资料”→“消息管理器”，如图3-69所示。

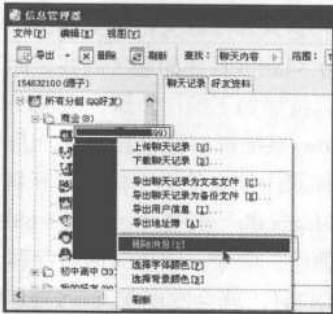


(2) 在弹出的消息管理器界面的左侧子窗格中选中的一个目标联系人，然后单击消息管理器窗口工具栏中的“删除”按钮，如图3-70所示。这样与指定好友进行聊天的所有记录内容都将被单独删除。

如果想同时将几位好友的聊天痕迹消除干净的话，那可以在图3-70所示的左侧子窗格中，借助Ctrl功能键将几位目标好友的头像图标逐一选中，然后再单击一下该窗口工具栏中的“删除”按钮即可。



【图3-69】打开消息管理器



【图3-70】删除与某位好友的聊天记录

【案例3-11】用QQ聊天保密箱加密想要保密的一段聊天记录。

目前市面上比较流行的QQ聊天记录保密的方法就是使用QQ聊天保密箱，用这个软件可以对自己的聊天记录加锁，别人没有解锁密码看到的聊天记录会是乱码或无法显示。

(1) 首先要从QQ聊天记录中提取想要保密的某一段聊天记录。打开“信息管理器”对话框，单击执行“导出”→“导出为.txt文档文件”命令，导出这段聊天记录，如图3-71和图3-72所示。



【图3-71】导出聊天记录



【图3-72】保存聊天记录到本地

(2) 保存好后在桌面上就会生成一个QQ号码.txt的文本文件，里面就是聊天记录。然后打开“QQ聊天保密箱”软件，单击执行“加密操作”→“打开原文本文件”命令，如图3-73所示。导入刚才保存的.txt文档，如图3-74所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 3 章 聊天黑客工具

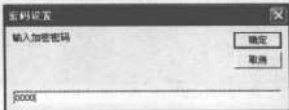


【图3-73】打开原文本文件



【图3-74】导入后的界面

(3) 单击执行“加密操作”→“另存为加密文件”命令，在弹出对话框中选择一个保存地点，并在“密码设置”对话框中输入密码，如图3-75所示。然后单击“确定”按钮，直到提示加密完成。



【图3-75】设置加密密码

(4) 完成加密后，该聊天记录文件就会被保存成为一个QQ聊天保密箱的专属文件，用其他方式无法打开，如图3-76和3-77所示。



【图3-76】QQ聊天保密箱专属文件



【图3-77】无法直接打开

(5) 如果要打开这个加密的文件，可以通过“QQ聊天保密箱”的解密功能来完成。单击执行“解密操作”→“打开已加密文件”命令，如图3-78所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图3-78】打开已加密文件

(6) 然后选择需要打开的已加密文件，输入自己设定的密码就可以看到加密后的聊天记录，如图3-79所示。



【图3-79】查看已加密文件

3.3 小结

在实时聊天工具使用中可能会遭遇到很多问题，受到盗号工具和破坏工具的攻击，特别是QQ，针对QQ的破坏工具是相当的多，所以在学习了本章之后对聊天工具的破坏应该有一个清楚的认识。

第4章

邮件黑客工具

电子邮件（E-mail）对上网的人而言，是如此的难离难弃。作为一种使用人数多的服务，就必定会有针对这种服务的黑客工具，无论作为商业机密窃取或者个人原因，E-mail的安全最值得担忧。本章将重点介绍各种邮箱破解工具、邮箱客户端软件破解工具、电子邮件攻击的方法，希望通过本章的学习，能帮助广大邮箱用户学会保护电子邮箱安全的方法。

本章要点

- ◎ 网页邮箱暴力破解的原理
- ◎ 邮箱客户端软件的使用以及破解
- ◎ 认识电子邮件攻击
- ◎ 邮箱密码设置

4.1 网页邮箱暴力破解

网页邮箱盗号工具一般可以分为三种，一种属于木马工具，记录访问过的页面的登录信息，发给指定邮箱；第二种是在线暴力破解工具；还有一种就是本章要着重讲解的暴力破解POP3账号。

4.1.1 暴力破解原理

暴力破解实际上就是试密码，一个一个去试，实际上是个很笨的破解方法，由于有了字典的帮助暴力破解使用起来也比较方便，一般黑客都有一个好用的字典。

4.1.2 用溯雪暴力破解邮箱密码

溯雪是一种在线暴力破解工具，它的使用并不复杂。

【案例4-1】使用溯雪破解邮箱。

(1) 运行溯雪程序，如图4-1所示。在区域1输入要登录邮箱的URL，然后单击键盘上的“Enter”键，打开登录窗口，在区域2也会出现页面表单的内容。



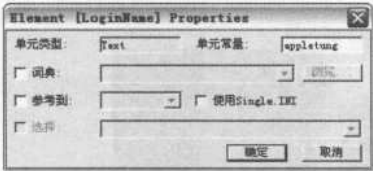
【图4-1】溯雪主界面

(2) 双击表单中的“LoginName”，在弹出的“Element [LoginName] Properties”窗口中，“单元常量”栏填入需要破解的用户名。由于破解的用户名已知，所以是常量，如图4-2所示。

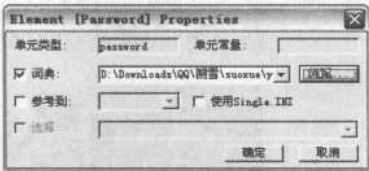
(3) 双击表单中的“Password”，在弹出的“Element [Password] Properties”窗口中，勾选“词典”选项，然后点击“浏览”按钮，选择一个破解词典，如图4-3所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 4 章 邮件黑客工具



【图4-2】输入用户名



【图4-3】选择密码破解词典

注意：溯雪自带了一些破解词典，如果这些词典不能满足需要，可以用词典生成工具，生成想要的词典。一般黑客都有一个比较好的词典。设置完成以后，表单会变成如图4-4所示的样子。

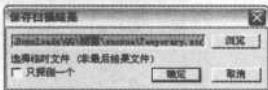
Element	Type	Content	Dictionary
<input checked="" type="checkbox"/> LoginName	password	apptung	
<input checked="" type="checkbox"/> Password	password		E:\Downloads\QQ\词典\passwords\passwords.dic
<input checked="" type="checkbox"/> Submit	submit	登录	
<input checked="" type="checkbox"/> domain	select		

【图4-4】设置完成

- (3) 选择菜单“运行”→“开始/重新开始”选项，如图4-5所示。
- (4) 在弹出的“保存扫描结果”窗口中单击“浏览”按钮选择保存的文件，如图4-6所示。
- (5) 单击“确定”按钮，会弹出“选择标记”窗口，选择一个错误标记，比如“域名错误”，然后单击“确定”按钮，如图4-7所示。



【图4-5】选择“开始/重新开始”选项



【图4-6】“保存扫描结果”窗口



图4-7选择错误标记

- (6) 单击“确定”按钮以后，此时开始暴力破解过程，状态栏会显示破解的进度，如图4-8所示。如果字典选择正确，就会破解出正确的密码。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图4-8暴力破解密码

4.1.3 轻松利用163邮箱破解器登录163邮箱

163邮箱破解器是破解163邮箱的黑客工具，通过它可以破解设置简单的163邮箱密码。

『案例4-2』使用163破解器破解163邮箱。

(1) 运行163邮箱破解器，弹出主界面，如图4-9所示，单击左上角第一个框中的“form”，在左上角第二个框中出现的“表元素”中单击“username”的“传递值”使之被选中，然后在“固定值”框中输入要破解的163邮箱的用户名，然后单击“定义”按钮。



【图4-9】163邮箱破解器主界面

(2) 刚才输入的163邮箱的用户名出现在“传递值”栏，单击“选用”按钮，如图4-10所示。



【图4-10】选择字典

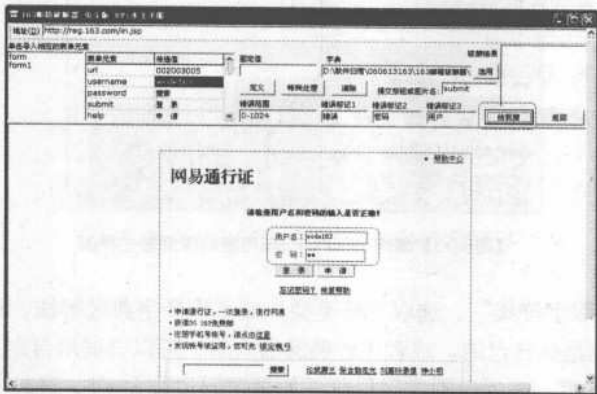
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵权阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(3) 弹出“打开”对话框，为破解选择一个字典，字典可以下载现成的，也可以自己做一个，将可能的密码写入记事本中保存起来，破解的时候就从字典依次提取出来试密码，一般黑客都有一个好用的字典。选择好字典之后单击“打开”按钮，如图4-11所示。



【图4-11】选择字典

(4) 单击主界面中的“给我搜”按钮，开始破解，破解成功后会将用户名和密码都显示在主界面中的“网易通行证”的用户名和密码框中，单击“登录”按钮就可以进入此163邮箱了。



【图4-12】破解成功

4.1.4黑雨 邮箱密码破解器破解POP3邮箱

与溯雪不同，黑雨是一款通过流行的pop3协议进行邮箱账号密码破解的黑客工具软件。黑雨利用“穷举法”进行远程暴力破解密码，它可以支持字符方式、自定义字符、字典方式、字串方式四种不同的方式进行密码计算。

它有四种算法：

- (1) 深度算法：这是一种很特殊的算法，如果你位数猜得准，就可以将时间缩短30%~70%。
- (2) 广度算法：此算法CPU占用比上面的方法多2%，速度快一点，但它是一种老式的算

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



法，现大多数类似功能的破解工具都采用它，对短小密码（3位以下）非常强。

(3) 多线程深度算法：如果你是K7、P3类的电脑则强烈推荐，理论上可以提高速度700%以上。

(4) 多线程广度算法：速度较快，如果你在局域网中或你上的是ADSL、Cable一类的网络，那你就会体会到它的快速。需要提醒的是：要验证用户名，一定要先登录服务器。选上字符方式和字串方式，再选一个算法，设定好后，就可以开始破解邮箱密码了。

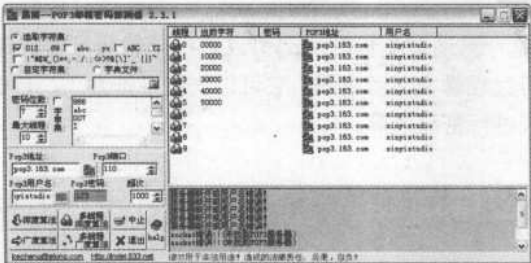
【案例4-3】使用黑雨破解邮箱。

(1) 运行黑雨——POP3邮箱密码探测器，如图4-13所示。在POP3地址栏填入要破解邮箱的POP3地址，比如网易免费邮箱的POP3地址是pop3.163.com，搜狐免费邮箱的POP3地址是pop3.sohu.com，但是不一定所有的都是pop3开头，例如电子科技大学邮箱的POP3地址是mail.uestc.edu.cn。POP3默认端口为110。填入需要破解的用户名。



【图4-13】黑雨——POP3邮箱密码探测器主界面

(2) 选择“选取字符集”，选取字符类型。或者选择字典破解法，选择字典的位置。如果你需要破解的邮箱是你自己的，或者比较熟悉的人的，可以尝试用自定义字符集，尝试的内容可以是生日、名字等。然后设置密码位数，如果密码位数大于5，建议使用大一点的线程。点击“深度算法”、“多线程深度算法”、“广度算法”或者“多线程广度算法”进行密码暴力破解，如图4-14所示。



【图4-14】开始暴力破解邮箱密码

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(3) 如果破解成功，就会在“密码”栏显示破解出的密码，如图4-15所示。



【图4-15】破解成功

4.2 破解邮箱客户端软件

本节以Foxmail软件为例，在简单介绍Foxmail之后，讲述使用Foxmail杀手获得Foxmail密码，以及Foxmail密码安全保护

4.2.1 Foxmail软件介绍

在邮件软件风起云涌的今天，一个短小精悍、功能强大的国产软件抢占了一席之地。这就是一个叫张小龙的中国人编写的邮件软件Foxmail。目前最新的版本为5.0版本。Foxmail可以收取多个邮箱的电子邮件。每个账户可以设定不同的密码，从而保护用户隐私。

4.2.2 用Foxmail杀手获得Foxmail账户密码

目前有很多针对Foxmail的密码破解软件，现在介绍一种，名叫Foxmail杀手，可以绕过密码，直接看到邮件。

『案例4-4』使用Foxmail杀手破解邮箱

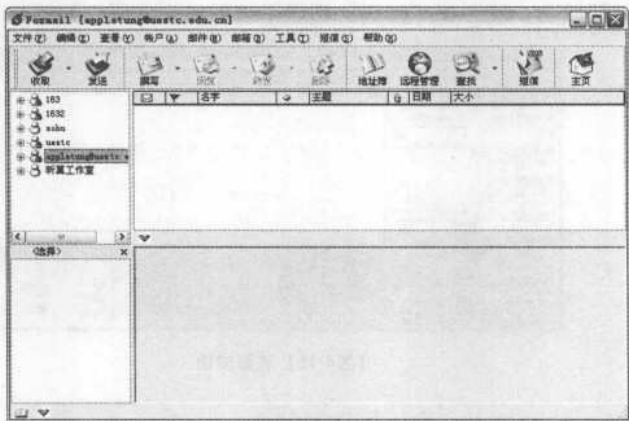
(1) 运行Foxmail杀手，弹出其主界面，如图4-16所示。



【图4-16】Foxmail杀手主界面

(2) 运行Foxmail，选择一个要查看的信箱，如图4-17所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

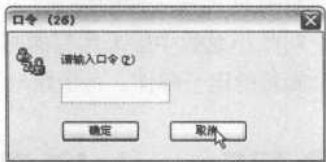


【图4-17】选择信箱

- (3) 使用“Alt+Tab”组合键切换到Foxmail杀手界面，在“左键窗口”按钮处，点击鼠标左键，此时你可以看见鼠标已经变成了Foxmail logo的形状，如图4-18所示。
- (3) 点住鼠标左键不要放，把鼠标拖动到Foxmail界面，在刚才选择的邮箱图标上放开鼠标左键，此时会弹出“口令”对话框，如图4-19所示。



【图4-18】在Foxmail杀手界面点击鼠标左键



【图4-19】“口令”对话框

- (4) 单击“取消”按钮，不用输入密码，查阅到该邮箱所有的邮件，如图4-20所示。



【图4-20】绕过密码查看到邮箱内容

4.2.3 Foxmail账户密码保护

1. 加密帐号

无论做什么事总是希望安全第一，可能你不想让别人在你离开时偷窥你的信件，那么给你的信箱加上口令就很重要了。选中你的用户名，鼠标右键单击，选择访问口令，在对话框中输入密码，再确认。另外，当启动Foxmail以后，输入信箱口令后口令将被存在内存中，那么当离开电脑而不关闭Foxmail时别人就可能再收一次信，很不安全。单击工具，找到清除内存口令，这一项可以消除在内存中的口令。

2. 加密邮箱

Foxmail允许为某个邮箱设置密码（主要是指为自定义邮箱设置密码，Foxmail的系统邮箱如收件箱等无法设置密码），以进一步的保护自己信息的安全。为此，只需选择需要加密的邮箱，然后执行邮箱菜单的加密命令，打开口令对话框并输入适当的密码即可。

4.3 电子邮件攻击

某一天，当你打开自己的电子邮箱，发现里面有一封陌生人发来的邮件，发信人ID看起来也没有任何规律可言。好奇心驱使你打开了邮件，但是你并没有发现任何有价值的内容。接下来的情况让你有些措手不及，因为你的邮箱很快被塞满了陌生人的邮件。于是你想收到的邮件却不知道被塞到了哪个地方。不必惊慌。这其实就是信息时代商战中经常见到的电子邮件攻击。电子邮件攻击是目前商业应用最多的一种商业攻击，它还有一个比较形象的名字叫做“邮件炸弹”。

4.3.1 电子邮箱信息攻击原理

邮件炸弹，简单的说是针对一个邮箱地址，狂轰烂炸般地发送大量垃圾邮件，从而达到攻击邮箱的目的。这种手段不仅干扰用户的电子邮件系统的正常使用，甚至还可能影响到邮件系统所在服务器的稳定，造成整个网络系统全部瘫痪。所以，电子邮件炸弹是一种杀伤力极其强大的网络武器。

电子邮件攻击有很多种，主要表现为：

(1) 窃取、篡改数据：通过监听数据包或者截取正在传输的信息，可以使攻击者读取或者修改数据。通过网络监听程序，在Winodws系统中可以使用NetXRay来实现。UNIX、Linux系统可以使用Tcpdump、Nfswatch（SGI Irix、HP/US、SunOS）来实现。而著名的Sniffer则是有硬件也有软件，这就更为专业了。

(2) 伪造邮件：通过伪造的电子邮件地址可以用诈骗的方法进行攻击。

(3) 拒绝服务：让系统或者网络充斥了大量的垃圾邮件，从而没有余力去处理其它的事情，造成系统邮件服务器或者网络的瘫痪。



(4) 病毒：在现在生活中，很多病毒的广泛传播是通过电子邮件传播的。I love you就是近年来最为鲜明的例子。

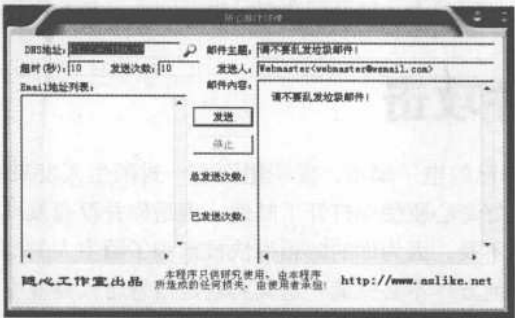
4.3.2 随心邮箱炸弹

随心邮件炸弹 v1.6，程序本身自带SMTP服务器，可以直接轰炸对方的邮件地址，快速高效。支持发送邮件地址列表；发送次数可自定义；DNS服务器可自定义为高速DNS地址，也可以取本机的DNS地址；发送人的MAIL地址可随意更改。

『案例4-5』使用随心邮件炸弹v1.6攻击邮箱。

利用Wsbomb进行Email炸弹攻击的操作步骤如下：

- (1) 首先运行Wsbomb，如图4-21所示。



【图4-21】Wsbomb界面

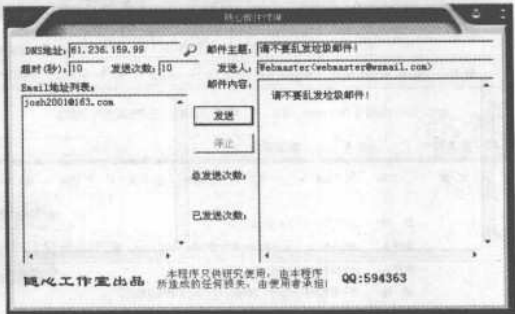
- (2) 填入DNS地址。DNS地址可以通过在运行中输入“cmd”启动MS-DOS，然后输入“ipconfig /all”命令，查看本机DNS，如图4-22所示。



【图4-22】查看本机DNS信息

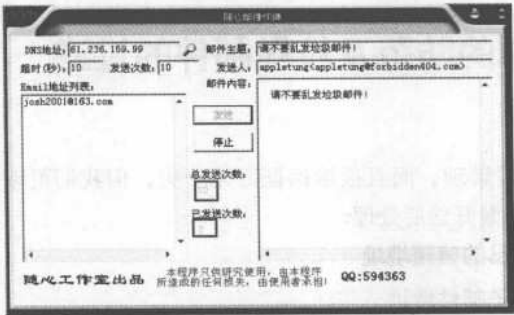
- (3) 输入需要发送的Email地址和邮件内容信息，如图4-23所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

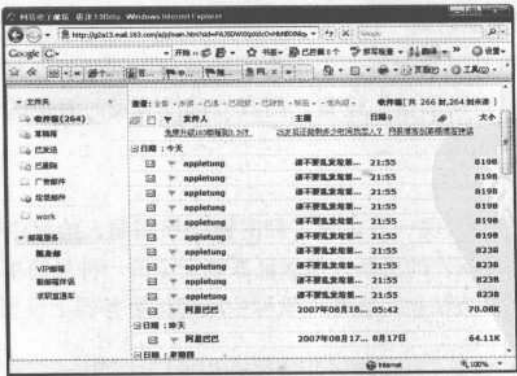


【图4-23】设置其余信息

(4) 单击“发送”按钮，就开始发送邮件，程序会显示总共发送的邮件次数和已经发送的邮件次数信息，如图4-24所示。这里选择的发送次数为“10”，打开邮箱，则发现已经收到了10封由Wsbomb发送的邮件，如图4-25所示。



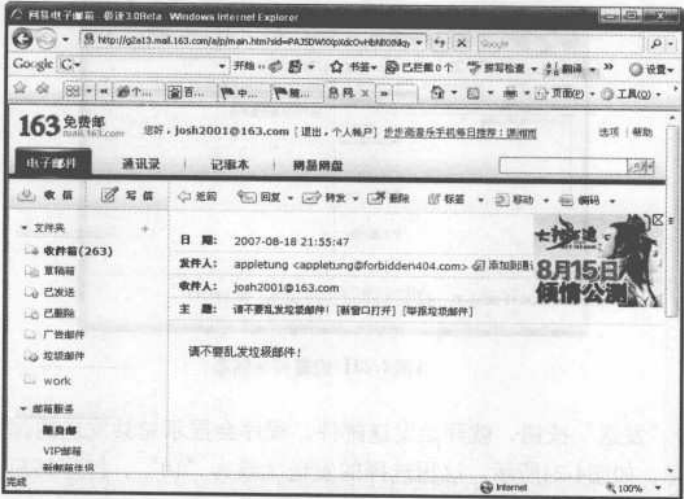
【图4-24】发送状态信息



【图4-25】发送成功

(5) 查看邮件内容，和先前设置的发送内容一致，如图4-26所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图4-26】邮件内容

4.3.3 邮箱炸弹的防范及垃圾邮件的过滤

1. 防范邮箱炸弹

邮件炸弹的防范比较繁琐，而且很难保证万无一失，但我们可以使用如下方法来尽可能地避免邮件炸弹的袭击和做好善后处理：

- (1) 不随意公开自己的信箱地址
- (2) 隐藏自己的电子邮件地址

例如将shy@163.com在输入时改成shy. 163.com，这样一来大家都知道这个实际上就是邮箱，但是一些邮箱自动搜索软件就无法识别这样的“邮箱”了。

(3) 谨慎使用自动回信功能

“自动回信”功能设计初衷很好，但也有可能被利用制造邮件炸弹。试想一下，如果接收和发送双方都设置了“自动回信”设置，而双方都没有及时看信的话，就会反复“自动回信”，造就了一颗邮箱炸弹。

(4) 打好补丁

在软件设计中，经常会出现一些意想不到的错误和漏洞，给程序带来安全性和稳定性方面的隐患。因此，经常保持对软件的更新，是保证系统安全的一种最简单也是最直接的办法。

防范邮箱炸弹的一个好方法就是在邮件软件中或邮件服务器上设置好防范项目。

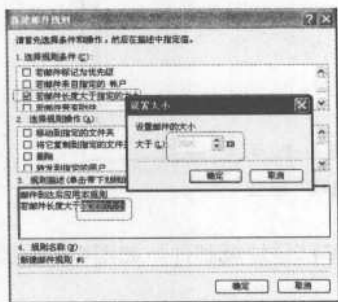
『案例4-6』Outlook Express的防范垃圾邮件策略。

- (1) 打开Outlook Express中单击“工具”，在弹出的下拉菜单中单击“邮件规则”→“邮件”，如图4-22所示。

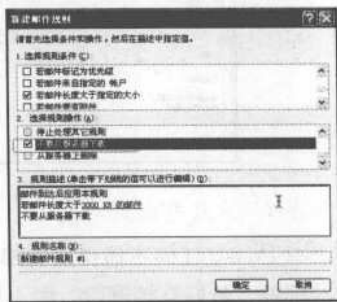


【图4-27】Outlook Express

- (2) 在弹出的“新邮件规则”对话框中勾选“规则条件”中的“若邮件长度大于指定的大小”，然后在“规则描述”中单击“指定的大小”，弹出“设置大小”对话框，在其中输入邮件大小的上限，例如3000kb，然后单击“确定”按钮，如图4-28所示。
- (3) 选择规则的操作，就是当收到的邮件大于限定之后怎么处理，勾选“不要从服务器下载”或者“删除”，如图4-29所示。

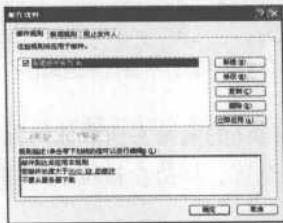


【图4-28】限制邮件大小



【图4-29】选择规则的操作

- (4) 根据信箱容量设置条件是大于3000kb，操作是“不要从服务器下载”，单击“确定”按钮，完成设置，如图4-30所示。于是只要是大于3000kb的邮件，就不会自动从服务器上下载，从而保护了邮箱。
- (5) 收到了邮箱炸弹之后，先打开一封炸弹E-mail，记下发信人的地址，然后登上邮件服务器，进入“邮箱配置”，设置“拒收过滤器”，把发炸弹人的地址输入到黑名单中，一旦收到这些人的信，就会自动在服务器上删除；设置“收件过滤器”，一旦邮件超过一定大小，也在服务器上删除。



【图4-30】完成规则设置

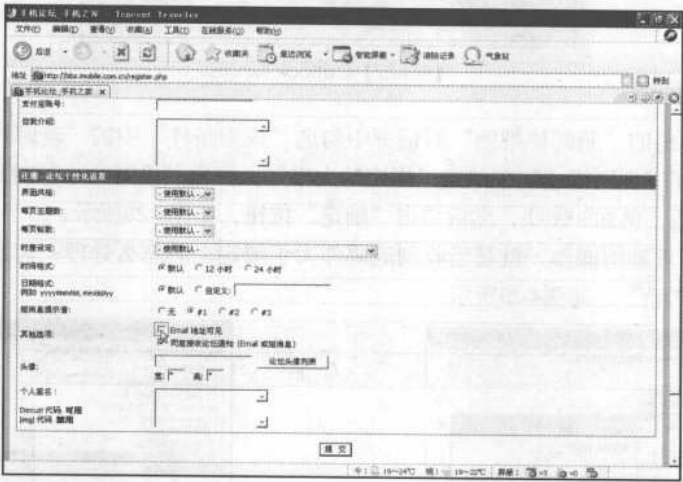


2. 防范垃圾邮件

(1) 防范垃圾邮件的准则

为了有效防止垃圾邮件，用户必须要遵照一定的策略和标准。这些标准是非常有效的。

①在互联网上的公众场合（聊天室，论坛）不要公布自己的任何邮件信息。如图4-31所示的就是我们在填写论坛注册信息的时候，最好把“E-mail地址可见”的选项滞空。



【图4-31】“把E-mail地址可见选项”滞空

②不要轻易回复任何不请自来的邮件，因为它们大多都是垃圾邮件。如图4-32所示对一些不请自来的邮件，最好直接删除，而不要进行回复操作。



【图4-32】不请自来的邮件

③不要登录并注册那些不值得信任的网站去获取任何服务，除非使用虚假信息。

④不要订阅一些不健康的电子杂志，以防止被垃圾邮件收集者收集。如图4-33所示是一些不健康的邮件的信息。

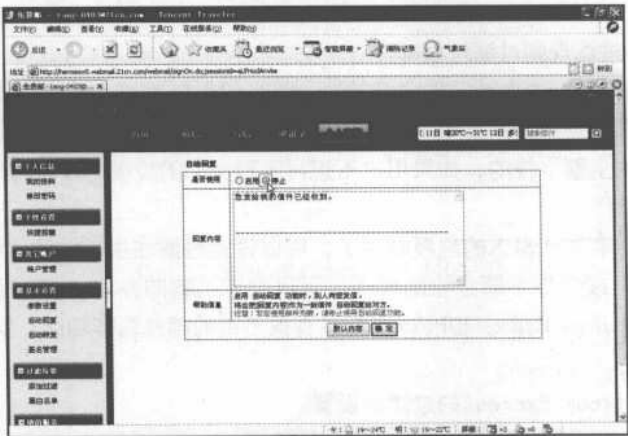
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 4 章 邮件黑客工具



【图4-33】不健康邮件

⑤谨慎使用邮箱的“自动回复”功能，它会让垃圾邮件确认这个地址的存在，后果更严重。如图4-34所示的邮件中的自动回复功能，最好采用“禁止”功能。



【图4-34】自动回复功能

⑥发现收集或出售电子邮件地址的网站或消息，请告诉相应的主页提供商或主页管理员，将你删除，以避免邮件地址被他们利用。

⑦建议用专门的邮箱进行私人通信，而用其他邮箱订阅电子杂志。

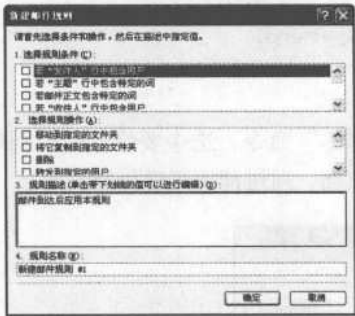
⑧不要轻易泄露自己的ISP信箱地址，如果不得不留下邮箱地址以方便其他网友与自己联系，可以采取一些变通的方式：如将xxx@163.com写成 xxx#163.com.这样网友会明白你的意思，而E-mail地址收集软件会将其视为非法地址而放你一马。

⑨使用好邮件软件的管理功能，网民们常用的Outlook express和Foxmail都具有不错的邮件管理功能，可实现邮件的过滤。

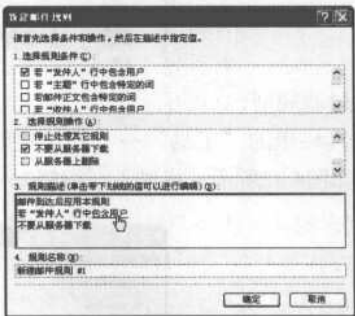
⑩使用专业的垃圾邮件清除软件。如Novasoft公司的Spamkiller软件，可以到下面的网站下载（<http://www.jetdown.com/down/soft/5285.htm>）和Unisyn software公司的SpamEx（邮件清道夫）等软件，如图4-35所示就是Spamkiller的操作界面。

件的处理方式，你可以拒收、删除信件也可以与文件夹结合使用，将信件自动保存在指定信箱。在“规则描述”规则说明中编辑相应的过滤条件，填入过滤字符串。最后就是填入“规则名称”，点击“确定”按钮建立过滤规则。例如：当用户希望拒收xxx@163.com的信件，并将所有来自pop@163.com的信自动保存到收件箱中的“friend”文件夹中（用户自建文件夹）。

(3) 可以将过滤规则第一项“选择规则条件”设置成“若‘发件人’行中包含用户”，在“选择规则操作”为“不要从服务器下载”，在“规则描述”窗口中点击“包含用户”，如图4-38所示。



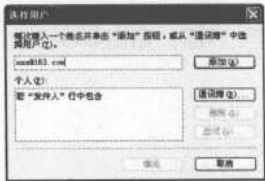
【图4-37】创建新邮件规则



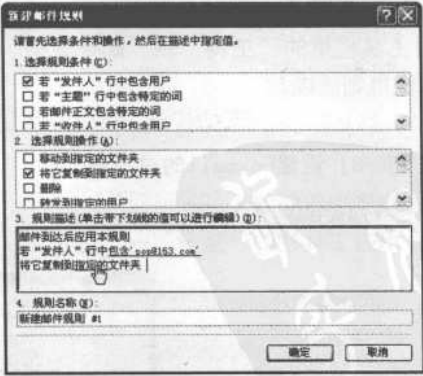
【图4-38】单击“包含用户”

(4) 在弹出的“选择用户”窗口添加用户“xxx@163.com”，如图4-39所示，然后单击“确定”使配置生效。

(5) 过滤规则第二若项“选择规则条件”设置成“发件人’行中包含用户”，在“选择规则操作”为“移动到指定的文件夹”。在“规则描述”窗口中点击“包含用户”，在弹出的“选择用户”窗口添加用户pop@163.com，然后单击“指定的文件夹”选项，如图4-35所示。

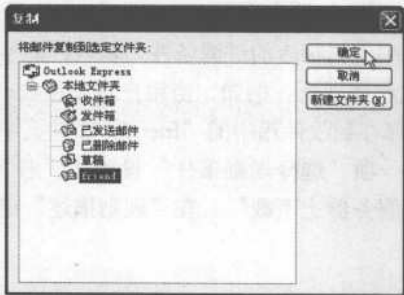


【图4-39】添加过滤用户



【图4-40】在“规则描述”窗口中点“指定的文件夹”

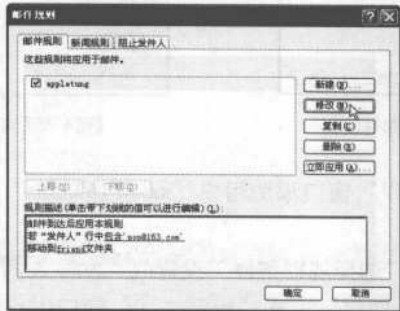
(5) 在弹出的“复制”窗口选择“本地文件夹/friend”，然后点击“确定”按钮，如图4-41所示，然后在规则名称中取名为“appletung”，再单击“确定”按钮即可。



【图4-41】选择“本地文件夹→friend”

2. 修改过滤规则：

单击工具栏里的“工具”→“邮件规则”→“邮件”命令，选中要修改的规则单击“修改”按钮，如图4-42所示，将进入“编辑邮件规则”页面，对过滤规则进行修改。



【图4-42】修改邮件规则

3. 删除过滤规则：

单击工具栏里的“工具”→“邮件规则”→“邮件”选中要删除的规则单击“删除”即可将该过滤规则删除。

『案例4-8』设置Foxmail的过滤器。

1. 过滤规则的创建：

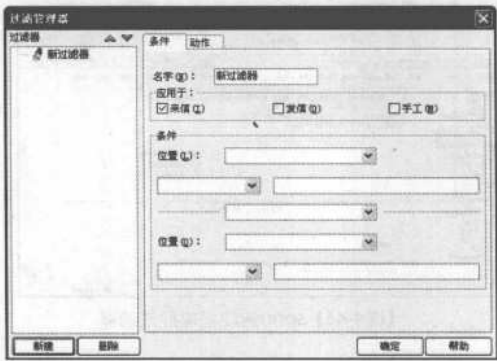
(1) 单击工具栏的“账户”→“过滤器”进入“过滤管理器”界面，如图4-43所示。



【图4-43】过滤管理器页面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(2) 单击“新建”按钮来建立过滤规则，填写所需的过滤内容，通过“条件”设定过滤规则，通过“动作”设置处理方式。如有不清楚的地方可点击右下方的“帮助”，如图4-44所示。

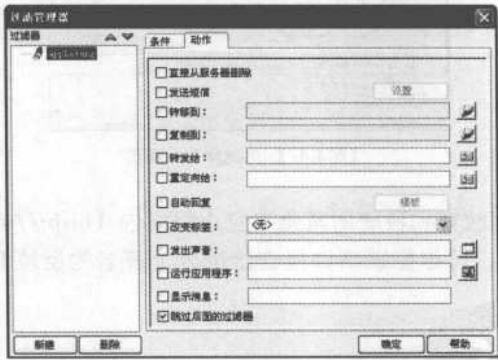


【图4-44】新过滤器创建页面

(3) 单击“确定”按钮建立过滤规则。

2. 过滤规则的修改：

单击工具栏的“账户”→“过滤器”命令进入过滤管理器界面。选中需修改的过滤规则进行修改，如图4-45所示。



【图4-45】对已有过滤器的过滤规则进行修改

3. 过滤规则的删除：

单击工具栏的“账户”→“过滤器”进入过滤管理器界面。选中需删除的过滤规则，点击左下角的“删除”按钮进行删除。

4. 报告垃圾邮件

阻止垃圾邮件的最佳地点是在你的ISP（Internet服务提供者），所以通过向你的ISP提交垃圾邮件报告可将垃圾邮件拦截在你的信箱之外。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



(1) 首选检查你的ISP是否提供垃圾邮件过滤器，如果有将使你根本就看不到这些讨厌的垃圾邮件，如图4-46所示Sohu垃圾邮件过滤器。



【图4-46】sohu的垃圾邮件过滤器

(2) 如果你的ISP没有提供垃圾邮件过滤器，你可以自己安装一个，或者注册一个过滤服务，由过滤服务先接收你的邮件，然后再转发到你的ISP帐号。ImaginNet (<http://www.imagin.net>) 便提供此项服务，如图4-47所示的该服务器的网页。



【图4-47】ImaginNet网页

(3) 也可以向中国教育和科研网紧急响应小组报告 (<http://www.ccert.edu.cn/>)。如果垃圾邮件是来自国外，可以把该事件报告给世界上著名的反垃圾邮件组织，如MAPS，SpamCorp等。

4.4 小结

本章主要围绕电子邮件这个话题，介绍了网页暴力破解邮箱密码，然后介绍了Foxmail的黑客软件，电子邮件的攻击原理、防范及垃圾邮件的过滤，希望对大家有所帮助。

第5章

网吧及网络游戏黑客工具

随着Internet的普及，网吧的数量越来越多，规模也越来越大，于是许多网吧都安装了专业的网吧管理系统。这些系统所带来的方便有目共睹，但越便捷的系统存在的安全隐患也越大，黑客们想出了很多破解这些管理系统的方法，有的甚至可以入侵网吧服务器，从而控制整个网吧。网吧的普及也推升了网络游戏的产业的发展，从暗黑破坏神、千年到龙族、传奇等，网游拥有众多的用户群，有时辛苦练级的账号，也会被网游黑客工具轻易盗取。

本章要点

- ◎ 网游账号隐患
- ◎ 网游账号安全保护
- ◎ 常见网游盗号软件
- ◎ 外挂作弊器
- ◎ 破解网吧集成管理工具
- ◎ 基本的网吧密码破解工具应用

5.1 网游盗号

网络游戏是一门产业，从暗黑破坏神、千年到龙族、传奇等，网游拥有众多的用户群，有时辛苦练级的账号，会被网游黑客工具，轻而易举盗得。

5.1.1 网游账号隐患

网络游戏中的安全隐患，一直都是广大网游者关心的话题。通常，网游账号被盗，都是存在着这样或那样的安全隐患。一般主要有以下因素：

1. 外挂

所谓外挂就是指某些人利用自己的电脑技术，通过改变网络游戏软件的部分程序，针对一个或多个网络游戏，制作而成的作弊程序。用户利用外挂这种作弊手段可以轻易得到其他正常用户无法得到、或必须通过长期运行程序才能得到的游戏效果。外挂的表现有很多种，有加速器、封包等，外挂最显著的特征就是带来不同于正常用户的游戏效果，使用它之后会比正常用户奔跑快、攻击威力加大、获得更多的游戏武器等。不过，外挂并不安全，经常使用外挂，网游账号的信息就会外泄，造成账号被盗。

2. 网吧

网吧里的系统都是“裸奔”的，基本上没有对任何木马病毒的防护，存在很大的安全隐患。所以在网吧玩游戏，登录那些你不熟悉的网站，很有可能中木马，不知不觉之间，你的网游账号就被盗了。

3. 安全邮箱

每个网游都设置有自己的安全邮箱，通常安全邮箱一泄露，网游账号也跟着泄露。所以，对于安全邮箱，要独立保护起来，才能保证网游账号泄露后，可用安全邮箱取回来。

4. 杀毒软件

经常玩游戏，没有杀毒软件无异于自杀。自己的电脑有必要安装一个强劲的杀毒软件，例如卡巴斯基，虽然启动慢点但是预防病毒和保护电脑效果不错。

5. 安全卡

大多数游戏都提供了这种功能，使用安全卡功能，可以为游戏安全再加上一把锁。而没有安全卡的网游，则很容易被盗号。

5.1.2 用魔兽世界黑眼睛盗取游戏密码

黑眼睛是盗取网络游戏密码的工具，它也是危害严重的网络游戏木马。黑眼睛可以同时截取美服、台服、欧服和国服魔兽世界的账号密码。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

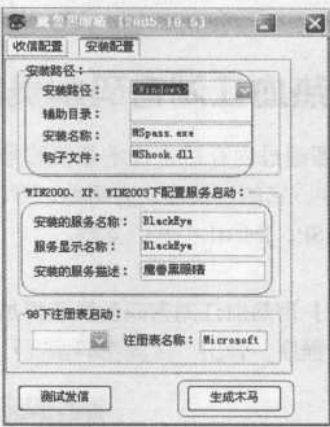
【案例5-1】利用魔兽世界黑眼睛盗取游戏密码。

该软件为一个ASP后门程序，专门收发游戏的账号信息。使用步骤如下：

- (1) 首先把ASP收信程序上传到支持ASP的空间，包括Post.asp文件。打开“魔兽世界黑眼睛”的主界面，如图5-1所示。
- (2) 可以看到有两个选项卡，在“收信配置”中，输入收入密码信箱、发送密码信箱、发送信箱Smt、及发送邮件主题，最重要的是把网站收信项的网址，在该文本框中，输入Post.asp文件所在的地址，输入结束后，单击“测试发信”按钮看看，是否成功。
- (3) 单击“安装配置”选项卡。在“安装路径”选项中，配置安装路径及安装名称、钩子名称，并设置好的它的启动服务名称，最后单击“生成木马”，即成功生成了盗魔兽世界账号的后门程序，如图5-2所示。

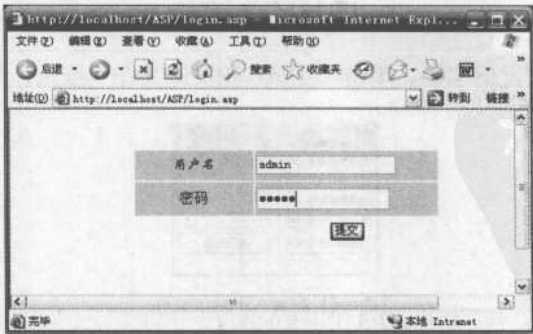


【图5-1】主界面



【图5-2】黑眼睛安装配置

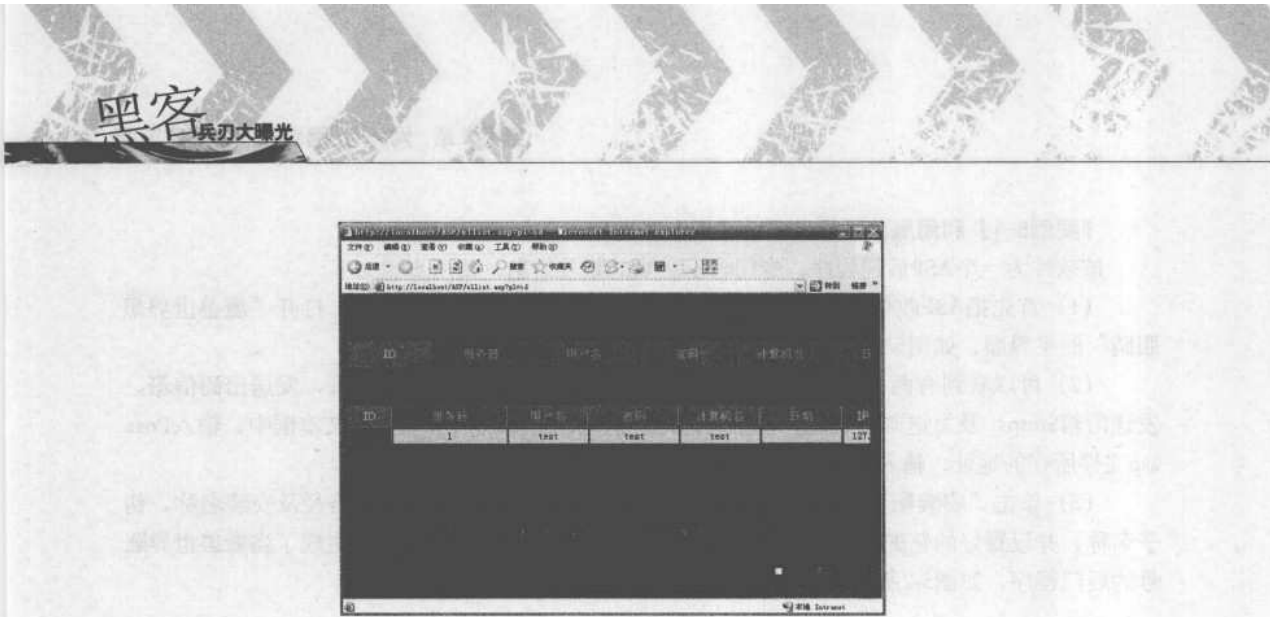
- (4) 登录到ASP程序集中，查看截取到的账号信息，如图5-3所示。



【图5-3】登录界面

- (4) 登录进来后，就可以看到已经截取到账号详细信息，如图5-4所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



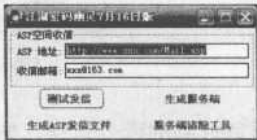
【图5-4】查看截取账号信息

5.1.3 用热血江湖密码幽灵获得热血江湖密码

该程序主要通过内存截密技术截获账号密码，无论是粘贴，复制，特殊字符，然后再发送到邮箱。其中，它的发信模式有两种，可以任意选择（空间，邮箱）。如果是空间，空间收信要求必须有ASP，JMAIL空间的支持。

【案例5-2】用热血江湖密码幽灵获得热血江湖密码。

(1) 运行程序，弹出“江湖密码幽灵”主界面，如图5-5所示。



【图5-5】程序主界面

(2) 首先生成ASP发信文件，单击“生成ASP发信文件”按钮，弹出“配置ASP发信文件”对话框，如图5-6所示。



【图5-6】配置ASP发信文件

(3) 在配置“ASP发信”对话框中，输入发信邮箱地址、发信邮箱账号、发信邮箱密码、发信SMTP设置等，设置好后，单击“生成ASP发信文件”按钮，即生成了发信文件，可以在目录下查看Mail.asp文件，如图5-7所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图5-7】 Mail.asp文件

(4) 生成发信文件后, 还要生成服务端, 才可以让木马运行起来。单击“生成服务端”按钮, 如没有问题, 即配置成功。

(5) 如果有问题,也可以选择“服务端清除工具”按钮,如图5-8所示清除服务端。



【图5-8】清除木马

5.1.4 用联众盗号机偷窥联众棋牌账号密码

联众游戏的盗号工具，准确记录联众大厅登录号码和密码，保存到指定文件和发送到指定邮箱。自带捆绑工具，将资料文件和必要的工作文件捆绑成一个独立的文件，通过发送在其他机执行，只要运行一次，即可自动安装。

【案例5-3】使用联众盗号盗取游戏账号。

该软件主要由以下几个文件组成，如图5-9所示。



【图5-9】主要文件

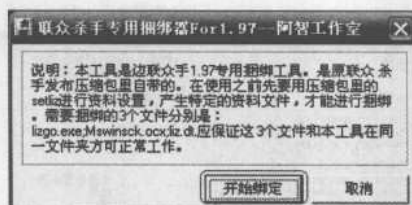
(1) 本机使用：运行SETLIZ程序，进行资料设置，如图5-10所示。选择本地保存路径，设置接收邮箱及邮箱用户名。



【图5-10】资料设置

(2) 设置成功后,运行“LIZGO.EXE”,运行时,正常的情况是没有任何反应的,运行后联众杀手就自动拷贝和安装,正常工作了,之后为了安全,可以删除所有解压的文件。

(3) 捆绑使用：同样的，首先也使用SETLIZ进行资料设置，如图5-10所示。设置成功后，会在当前目录下生成一个用户信箱资料文件：liz.dt。再运行捆绑工具：LIZBIN.EXE，进行捆绑，如图5-11所示。



【图5-11】捆绑器

(4) 捆绑成功后，在当前目录下生成一个名为：“OHGAME.EXE”的可执行文件。这个文件已经包含了你的邮箱资料信息和所有联众杀手的工作文件，可以在任何一台主机运行使用。只要运行一次（运行时没有任何提示）就可以自动安装和工作。这样可以发送给你的目标人，只要对方执行，就可以在对方机上自动安装联众杀手，并依据你当时设置的邮箱信息，将密码信息发送给设置的邮箱。

5.1.5 网游账号安全保护

对于网游账号的保护，大家要从自己的爱机做起，为了你账号的安全，以下是一些基本的设置，只要时时有防范之心，加上良好的用“脑”习惯。可以为网游账号的安全再加一把锁。

- (1) 请将IE的“Internet选项”的“高级”设置为“恢复默认设置”。
 - (2) 不要安装和下载一些来历不明的软件，特别是一些所谓的女神外挂程序。
 - (3) 不要随便打开来历不明邮件的附件。
 - (4) 安装最新杀毒软件，并定时升级病毒库。
 - (5) 在网吧上网时，小心网吧的计算机上安装有记录键盘操作的软件，或被安装了木马。使用网吧计算机时，需先按“Ctrl+Alt+Del”三个键，看看是否有来历不明的程序正在运行，如果有，则立即将该程序结束。
 - (6) 尽量避免将游戏账号暴露在公众论坛和其他网站。
 - (7) 用户在设置密码时，尽量复杂一点，最好设置为八位数以上的字母、数字和其他符号的组合。
 - (8) 不要使用可轻易获得的自己的信息作为密码。这包括生日、身份证号码、手机号码、你所居住的街道的名字等等。
 - (9) 经常更换密码，因为八位数以上的字母、数字和其他符号的组合也不是无懈可击的。
 - (10) 申请密码保护，也就是设置安全码，安全码不要和密码设置一样。如果你没有设置安全码，那么别人一旦破解你的密码，就可以把你的密码和注册资料（除证件号码外）全部修改。
- 最后就是要经常性地打操作系统补丁和升级病毒库文件和防火墙。

5.2 网游作弊

网游作弊，即是通过网游破解外挂，模拟鼠标和键盘动作或截取服务器数据封包进行修改，让玩家在最短的时间内获得最大的利益，在网络游戏中达到加速，不死或无敌的游戏状态。

5.2.1 外挂作弊器简单介绍

早期图形网络游戏（如uo、kok）的外挂说是出于善意的，外挂机器人只是代替线上玩家进行某些重复性动作，以达到长时间在线“练功”的目的，可以使一些忙于工作的人也能够享受到网络游戏的乐趣，网络游戏服务商对此也是睁只眼，闭只眼，因为外挂并没有对网络游戏规则造成太大的冲击，而如今，外挂已经不仅仅是重复性机器人而已。如“加速器外挂”可以大幅度修改客户端id的移动速度；“经验外挂”可以在游戏中向服务器发送npc本身xx倍的经验封包，以达到迅速成长的效果；更有甚者可以对服务器端的id或物品进行属性修改……网络游戏蒸蒸日上，而网络外挂也是如火如荼，似乎网络外挂与网络游戏的争端从有网络游戏就开始了，越是玩家聚集的游戏，外挂现象就越是严重，游戏外挂软件的多寡已经成为评价一个网络游戏成功与否的标准。甚至有玩家戏称：“没有外挂的游戏是网络垃圾”。当然这种观点有失偏颇，但外挂软件的确从另一个层面反映了网络游戏的受众程度。一个网络游戏，玩的人多了，外挂就会紧跟着来。《龙族》、《魔力宝贝》、《天使》、《传奇》等游戏无一幸免。奇迹的外挂似乎来得更快，快到点卡还未上市，外挂卡已经开始卖了。外挂软件给部分玩家带来刺激与兴奋之后，也破坏了游戏规则，这类的外挂已经严重影响了游戏的公平性，致使其他玩家无法与使用外挂的玩家进行抗衡，于是越来越多的玩家离开了游戏，网络游戏的运营商也逐步丧失了市场。因此外挂软件损害了玩家的利益也损害了运营商的利益，从某种程度上说也破坏了网络经济的健康发展。

5.2.2 用记牌器轻松记牌

1.QQ斗地主记牌器

QQ斗地主是时下流行的牌类游戏，QQ斗地主记牌器可以帮助玩家记录未出现过的牌，以及计算剩下的牌，以达到作弊的目的。

首先打开“QQ游戏”大厅，选择斗地主后，开始游戏之后，运行“QQ斗地主记牌器”，注意：在斗地主游戏没有开始之前，打开记牌器没有任何作用，打开记牌器后，出现主界面，如图5-12所示。

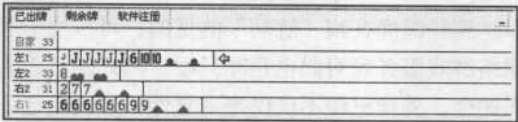


【图5-12】QQ斗地主记牌器

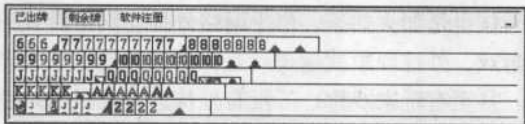
界面中列举了斗地主中所有的牌，并且牌上对应了数字或空格。比如4上面的数字4就是说明了除了玩家自己手中没有4，四张4全部在其他玩家手中，5上面的空格说明除玩家自己手上的5以外，其他玩家手中已经没有5了。

2. 联众保皇记牌器

打开“联众保皇”主界面后，运行“联众保皇记牌器”，弹出其主界面，如图5-13所示。默认为已出牌界面，可以查看自己和其他玩家的出牌情况。选择剩余牌按钮，会显示所有玩家手中剩余的牌的总和，如图5-14所示。



【图5-13】联众保皇记牌器查看已出牌界面



【图5-14】查看剩余牌界面

5.2.3 CS作弊器及反作弊器

1. CS的工作原理

当你玩CS的时候，你的电脑成为一个客户端(Client)。客户端负责收集你的键盘和鼠标指令，并绘在屏幕上。客户端和服务端相连。服务器注意所有客户端的状态。它发给客户端信息，告诉它每个人在哪里，在做什么。

客户端由两部分组成，引擎和客户端MOD。引擎处理和服务器的连接，在屏幕上绘图，并获取键盘和鼠标输入的信息。MOD部分处理和你玩的某个特定游戏相关的事情。每个游戏都有自己的MOD。如果你装了HL和CS，那么就会有一个HL的MOD，还有一个CS的MOD。但是只会有一个引擎。所有的MOD都使用相同的引擎。

引擎和MOD互动使你机子上的游戏顺利运行。大多数作弊软件的原理是把自己楔入引擎和MOD之间。引擎和作弊器“对话”，作弊器再把信息传递给MOD。同样，MOD和作弊器“对话”，作弊器再传给引擎。引擎和MOD仍然相关联，表面上看一切都好，其实两者实际上在通过作弊软件“交流”。这些作弊软件通常被叫做“客户端钩子”(“clienthooks”)。

2. 作弊器原理

大多作弊器都可以看作是CS的一个外挂程序，作弊器的运行方式从发展轨迹来说经历了

三大方式：

- (1) 作弊器早期阶段是通过程序使得CS在启动的时候，不去执行CS游戏本身固有的动态链接文件，而转去执行作弊程序锁提供的作弊功能链接文件。这种方式的作弊在早期比较多，但是当反作弊程序大行其道的时候这种方式逐渐消亡，因为它太容易被反作弊程序侦测到。
- (2) 最为强大的运行方式，作弊程序将尽全部可能独立运行，用自己独立的构架，独立的console，独立的菜单。通过侦测内存、监视游戏运行来得到游戏数据，将外挂程序与CS程序本身的瓜葛降到了尽可能低的程度。此种作弊方式是现在和未来相当长时间内作弊的主流。对于此种作弊，反作弊的难度较大。
- (3) 通过BUG来实现，多半是通过驱动的对号缺陷，再加上作弊程序对对应BUG的激活从而实现透视等效果。可以说这种方式对反作弊来说最为困难，CheatingDeath的作者也不断根据BUG发放最新补丁，很多朋友发现一进入CS某些版本游戏就有CODE错误，有一些就是因为CD对驱动系统要求过于敏感，一般更改一下驱动可以解决。

【案例5-4】使用作弊器CCA Hook V2.0实现暴力模式。

- (1) 双击它的主程序“CCA.EXE”，第一次进入游戏时，需要查找CS程序所在的目录。如图5-15所示。



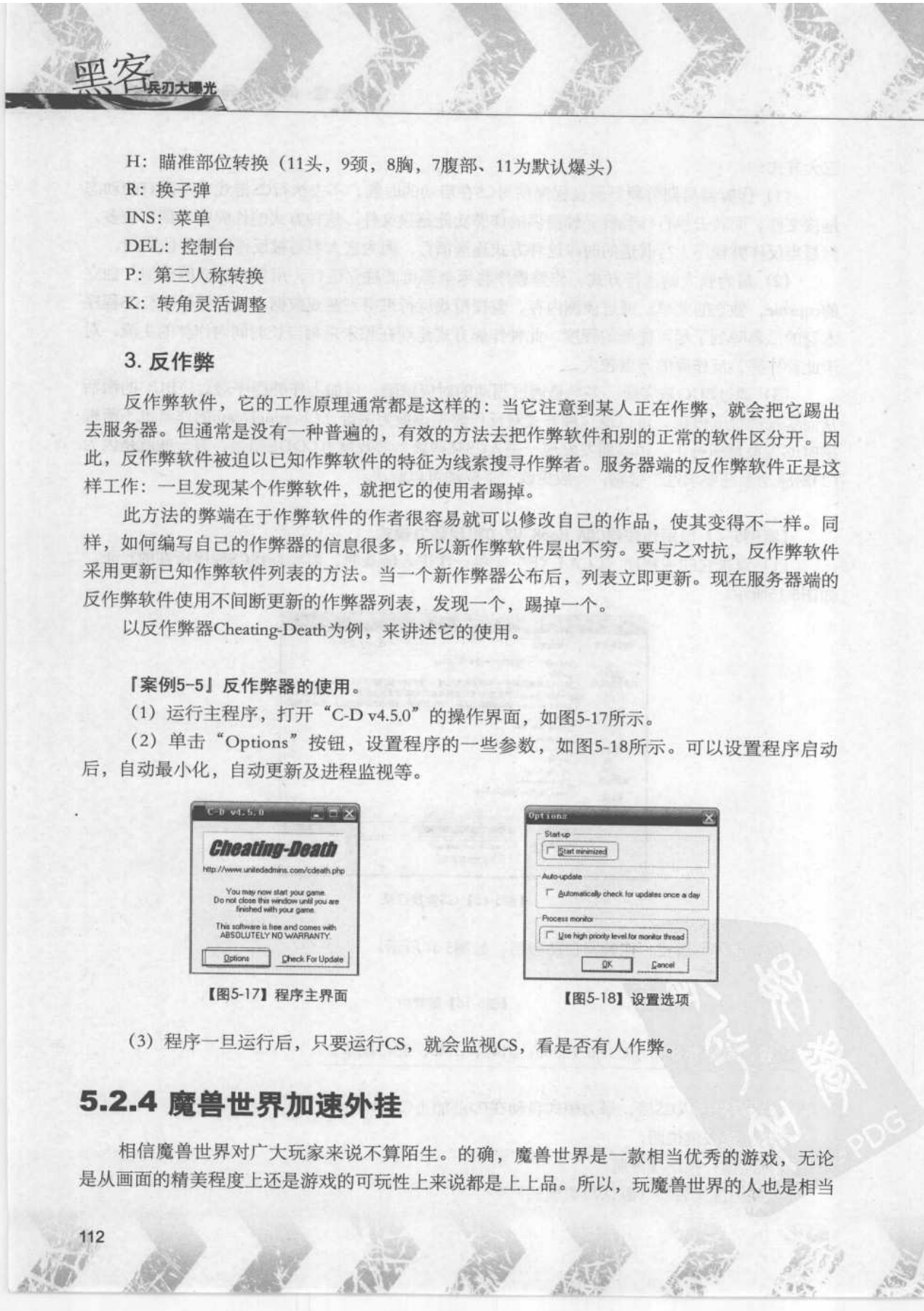
【图5-15】CS查找目录

- (2) 进入CS游戏，作弊器自动激活，如图5-16所示。

【图5-16】游戏中

注意：该作弊适用于CS1.6 V3266，3147，2148，3213版本。

- (3) 通常进入CS后，暴力模式自动在ID前加上C.C.A队标。
它的一些按键说明：
鼠标左键：按路线冲刺
L：暴力温柔转换（默认温柔模式）



- H: 瞄准部位转换 (11头, 9颈, 8胸, 7腹部、11为默认爆头)
- R: 换子弹
- INS: 菜单
- DEL: 控制台
- P: 第三人称转换
- K: 转角灵活调整

3. 反作弊

反作弊软件，它的工作原理通常都是这样的：当它注意到某人正在作弊，就会把它踢出去服务器。但通常是没有一种普遍的，有效的方法去把作弊软件和别的正常的软件区分开。因此，反作弊软件被迫以已知作弊软件的特征为线索搜寻作弊者。服务器端的反作弊软件正是这样工作：一旦发现某个作弊软件，就把它的使用者踢掉。

此方法的弊端在于作弊软件的作者很容易就可以修改自己的作品，使其变得不一样。同样，如何编写自己的作弊器的信息很多，所以新作弊软件层出不穷。要与之对抗，反作弊软件采用更新已知作弊软件列表的方法。当一个新作弊器公布后，列表立即更新。现在服务器端的反作弊软件使用不间断更新的作弊器列表，发现一个，踢掉一个。

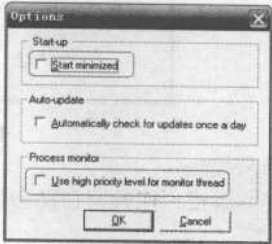
以反作弊器Cheating-Death为例，来讲述它的使用。

【案例5-5】反作弊器的使用。

- (1) 运行主程序，打开“C-D v4.5.0”的操作界面，如图5-17所示。
- (2) 单击“Options”按钮，设置程序的一些参数，如图5-18所示。可以设置程序启动后，自动最小化，自动更新及进程监视等。



【图5-17】程序主界面



【图5-18】设置选项

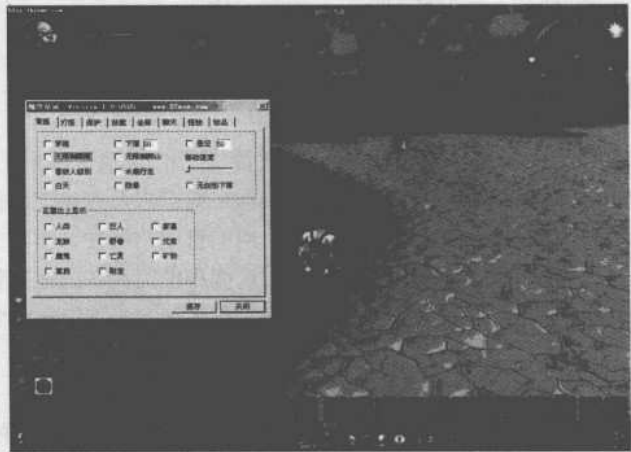
- (3) 程序一旦运行后，只要运行CS，就会监视CS，看是否有人作弊。

5.2.4 魔兽世界加速外挂

相信魔兽世界对广大玩家来说不算陌生。的确，魔兽世界是一款相当优秀的游戏，无论是从画面的精美程度上还是游戏的可玩性上来说都是上上品。所以，玩魔兽世界的人也是相当

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的多。当然，其中也少不了一些需要用外挂来辅助的玩家，现在就给大家介绍一下当下魔兽世界比较流行的外挂——魔兽皇冠，如图5-19所示。



【图5-19】魔兽世界皇冠外挂

- (1) 运行Crown.exe，将所有文件解压到同一文件夹。
- (2) 将魔兽世界游戏设定为窗口运行模式。窗口模式可以在游戏里面系统菜单里的视频设置里设定，也可以在游戏快捷方式里加上“-windowed”，如“C:\World of Warcraft\wow.exe”-windowed。
- (3) 运行解压目录Crown里的WowCrown.exe，不要关闭魔兽皇冠的主窗口，然后进入游戏里面，按F12键呼出即可。

功能介绍：

- (1) Disable Hotkeys：关闭热键。
- (2) No Fall Damage：高空掉落不掉血。
- (3) Mountain climb：无阻爬山（任何高山都可以爬上去）。
- (4) Lock Speed：速度锁定(例如：骑在马上然后点击Lock Speed后下马行走速度跟骑马一样)。
- (5) Zero Gravity：飞天（建议不要用）。
- (6) Teleport Plane：浮空（建议不要用）。
- (7) Follow NPC：跟踪NPC。

左边栏目为瞬间移动。

5.3 突破网吧管理工具

众所周知，Windows的系统安全性非常脆弱，应用在公共场合的Windows系统更是容易被用户破坏，经常重装Windows系统成了不少经营者无可奈何的日常工作。于是现在的网吧大多装有网吧管理工具，帮助网管人员解决网络维护问题，增强系统的安全性。使用较多的网吧管

理工具有美萍安全卫士、万象网管专家等。

黑客当然不会甘心被这些管理工具拒之门外，于是想出很多破解网吧管理工具入侵网吧系统的办法。这一节我们介绍破解网吧管理工具的软件。

5.3.1 跳过管理验证 Pubwin4.3修改程序

Pubwin系列产品主要用于网吧、学校等收费机房的管理，目前已经发布的最高版本是Pubwin2007。Pubwin 2007是基于广泛征集网管和业主的需求及建议之上研发的，满足网吧使用及管理需求，具备高度的安全性能；灵活部署、集中管理的特性；丰富的商业策略；严谨与高效的业务流程设计；低资源占有率及高速的启动速度和便捷高效的配置管理等；融入众厂商产品用户使用习惯并结合免费的带有虚拟还原功能的迅闪2007，不但具有强大功能，而且软件容易上手和使用。

Pubwin 2007系统特点：

(1) 多级用户权限控管——对网吧各级别操作用户分别设置不同的操作权限，操作及管理更加清晰，权责更加明确。

(2) 软件极性贴心设计——人性化的界面设置、简单便捷的向导式初始配置、通俗易懂整注释等提示语言，清晰明了的各种提醒和查询信息，多重的自定义设置功能等做到易上手、易于使用、便于管理。

(3) 融入综合使用习惯——融入市场上众多厂商产品的使用习惯，便于网吧更加人性化的管理及顾客更多种需求。

(4) 企业级平台——采用基于Web服务的分布式体系结构，建立在高性能的数据库SQL Server和J2EE容器Tomcat和安全、稳定、可扩展的Apache之上，能够支持Linux和Windows等多种操作系统。企业级构架使Pubwin 2007拥有可靠与强大的处理能力，完全能够胜任超大规模网吧的需求。

(5) 防破解、防木马——Pubwin 2007完善 Pubwin EP先进的Genfs技术，从操作系统核心入手，从根本上解决了网吧破解难题；Pubwin 2007优化提高原Pubwin EP内嵌的杀毒引擎功能，通过自动更新非法程序库，有效防止各种盗号木马行为，进一步加强网络安全性，为顾客创造了良好的上网环境。

(6) 强大的安全保障——网络通讯全面采用数字证书认证体系，具有与网上银行同等的的安全级别；基于角色的权限管理允许灵活定制管理权限；具有完备的数据保密、备份、灾难恢复等机制，保证数据高度安全可靠。

(7) 灵活的部署——通过将核心服务与操作的分离，允许部署任意多个具有完全功能的操作点，可以通过Web管理界面实现远程访问。

(8) 支持丰富的商业策略——从应有尽有的促销手段到无所不能的价格方案， Pubwin 2007帮助客户从容应对激烈的市场竞争。

(9) 严谨与高效的业务流程设计——Pubwin 2007业务数据遵循财务准则设计，严谨、规范；众多独到的设计不仅方便顾客使用也大大减轻了服务员的工作强度。

(10) 集中管理能力——将配置、升级等任务集中到服务器处理，使管理工作大量减少，变得高效。

(11) 完备的连锁管理功能——秉承Pubwin.net强大的连锁体系，优化完善Pubwin EP高效实现储值通用、结算、经营策略下发等连锁功能，付出极低成本即可实现中小型连锁网吧管理。众多独到的设计不仅方便顾客使用也大大减轻了服务员的工作强度。

(12) 易于使用与维护——Pubwin 2007充分考虑了不同层次使用者的接受能力，服务员经过10分钟简单培训就能掌握，管理人员则拥有众多工具和方法用于简化管理与维护。此外，为了帮助用户尽快熟练掌握Pubwin 2007的应用，Pubwin 2007新加入清晰明了的向导式配置，做到让用户可在最短时间内完成软件的基本配置及使用，新浩艺公司还提供了多种方式的培训和技术支持。

(13) 与公安、文化监控系统的整合——与国内大部分公安与文化监控软件实现了无缝衔接。

利用Pubwin4.3修改程序可以跳过Pubwin4.3网吧管理验证工具，取消许多上网限制，并且可以免费上网。

【案例5-6】使用Pubwin4.3修改程序。

(1) 首先将Pubwin4.3修改程序下载到本地，该修改程序包含两个文件：Pubwin.exe和Pubwin.pub。下载下来以后不要急于使用，首先要弄清楚Pubwin4.3的安装路径。

通常网吧会将其安装在默认目录：C:\Program Files\Hintsoft\Pubclt下，部分网吧安装在C:\Pubwin4，可以通过搜索文件名Pubwin.exe来找到路径。

(2) 找到路径后，将Pubwin.exe和Pubwin.pub两个文件复制到该目录下，覆盖原来的文件。如果Pubwin正在运行，可以利用冰河等黑客工具把Pubwin进程终止。

文件复制成功，Pubwin4.3也就破解成功了，破解后Pubwin的管理员密码会被清空，或者是任意密码。等待5秒钟左右，Pubwin会自动再次启动，界面如图5-20所示：



【图5-20】pubwin4.3主界面

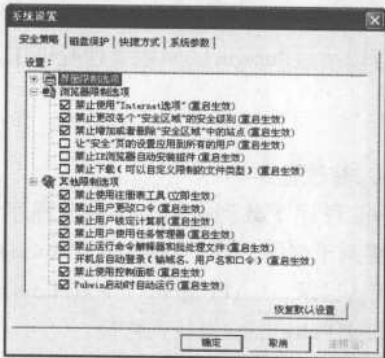


(3) 现在看看密码被清空了没有。右键点击系统任务栏中的Pubwin图标，选择“系统设置”，这时系统会要求用户输入管理员口令，图5-21所示。



【图5-21】Pubwin口令验证窗口

(4) 直接点击“确定”按钮，如果没有破解，系统将提示口令错误；但是现在不会了，单击“确定”即可打开“系统设置”对话框，图5-22所示。



【图5-22】Pubwin系统设置窗口

(5) 破解后进入“管理工具”将一些常见的限制取消，然后退出程序（右键点击任务栏图标，选择“退出系统”）。现在可以结账下机了，在前台看见这台计算机是闲置的，但是你仍然可以使用它正常上网。

5.3.2美萍9.0密码破解器

美萍安全卫士是一款实用的网吧、机房安全保护、计费管理软件，它实现了硬盘文件保护、远程控制、限时、定时运行计算机、应用软件运行限制等多项功能，被广泛适用于网吧。

美萍安全卫士的安全防护功能充当了电脑的保护神，它完全屏蔽了原来windows操作系统的界面，用户只能运行由“美萍安全卫士”事先选定的软件。另外美萍安全卫士还具有强大的管理功能，如计时计费、限时、历史记录等，如果配合“美萍网管大师”使用能实现利用一台管理机远程控制整个网络内的所有计算机。包括对任意机器进行开通和停止，暂停，关机热启动等操作，是网吧管理员不可或缺的利器。

“美萍9.0密码破解器”可以全面消除美萍安全卫士9.0密码，解除它对计算机及应用程序运行的多种限制。

【案例5-7】使用美萍9.0密码破解器破解密码：

“美萍9.0密码破解器”的使用十分简单，程序主界面如图5-23所示：



【图5-23】美萍9.0密码破解器主界面

(1) 清空密码：直接点击“清空密码”按钮，该破解器将自动把美萍安全卫士的密码设置为空。

(2) 解除限制：美萍安全卫士可以禁止用IE访问盘符、禁用98工具栏、禁止IE访问某些网站、屏蔽F3快捷搜索功能、禁止编辑注册表和禁用IE下载功能。

利用“美萍9.0破解器”能够轻易解除这些限制。用户只需要选中主界面中要解除的限制项前面的复选框，然后单击“保存设置”按钮即可。

(3) 解除自动运行：系统开机时，美萍安全卫士会随系统启动而自动运行，单击“解除自动运行”按钮后，下次启动系统时，就不会自动运行美萍安全卫士。

5.3.3 万象2R最新版破解器

万象网管专家是一款集计费、网络管理、商品销售等多功能于一体的网络计费管理平台。目前最新版本为2006。

2006针对2004进行了全面的改造和扩展：可以针对网吧情况，挂接任意多个收银点，上下机可以在任一收银点进行，真正方便用户；数据处理与收银点彻底分离，避免了收银机出现故障而引起数据破坏，2006采用UDP协议，从而避免了使用IPX协议脱管现象；内置网吧超市系统，顾客在上机过程中即可轻松选购商品。这是一套真正适用于大型、超大型网吧的管理系统。

万象网管专家的主要优点有：

(1) 功能模块分离：2006分为数据库、中心服务器程序、收银端程序、客户端几个部分，计费服务程序与数据库相连，专用于费用计算及各种命令的集中处理，而收银端仅仅起到信息显示及接收用户的操作指令的作用；所有数据全部保存在数据库及计费服务器上，收银端不保存任何数据，这样，在收银端出故障时，可以立即找到另一台机器安装收银端，对营业不产生任何影响。

(2) 大型网吧的理想选择：2006专为大型网吧设计，可以轻松管理超过2000台以上的电脑。

(3) 多收费机管理：在搭建好服务器之后，就可以任意挂接收费机（当然，收费点需要通过操作员用户、密码登录），且每个收费机都可以管理整个网吧的电脑。

(4) 通讯安全可靠：在万象以前的版本中，一直是采用IPX协议进行管理的，但对于网



络环境不太好的网吧，IPX容易产生脱管问题；因而，在2006中采用了UDP协议，使网吧通讯更加可靠，并能轻松实现跨网段管理。

（5）跨区域换机：万象网管2006已经可以支持跨区域换机了，会员卡和临时卡都可以在费率不同的区域任意换机。

（6）会员卡一卡多上：会员卡只要余额足够，就可以在多台机器上登录相同的会员卡，多台机器对会员卡同时扣费。

【案例5-8】使用“万象2R最新版破解器”。

“万象2R最新版破解器”可以破解万象网管专家R12版本，清除常见的上网限制。“万象2R最新版破解器”运行界面如图5-24所示：



【图5-24】万象2R破解器主界面

“清空所有密码”：单击该按钮将万象网管专家的所有密码设置为空，这样用户就可以进入万象网管专家管理功能，修改对系统所做的所有设置。

“去除启动运行”：禁止万象网管专家在系统启动时自动运行。

“主页设置”：选中该功能对应的复选框，“保存设置”后将会把浏览器主页修改为破解器中指定的页面。

“打开我的电脑”：使用了万象网管专家的客户主机，用户不能打开“我的电脑”，但是选中了这个复选框后，用户完全可以摆脱万象的限制，随意查看和修改“我的电脑”中的内容。

事实上，该破解器的操作非常简单，各个选项的功能从选项名就能看出来，这里就不再赘述。

5.3.4 网吧管理集成破解器

“网吧管理集成破解器”可以破解多个网吧集成管理工具：方竹网吧集中管理之王、方竹网吧管理和美萍安全卫士网吧管理工具，使用方法也非常简单。图5-25所示为“网吧管理集成破解器”程序界面。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图5-25】“网吧管理集成破解器”主界面

该集成破解器可以获得、清空、更改方竹网吧集成管理之王的密码。

【案例5-9】使用“网吧管理集成破解器”破解“方竹网吧集中管理之王”。

(1) 取得密码。直接单击主界面上的“取得密码”按钮，管理之王的密码就会显示在主界面对应的文本框中，图5-26所示。



【图5-26】获得“方竹网吧集成管理之王”密码

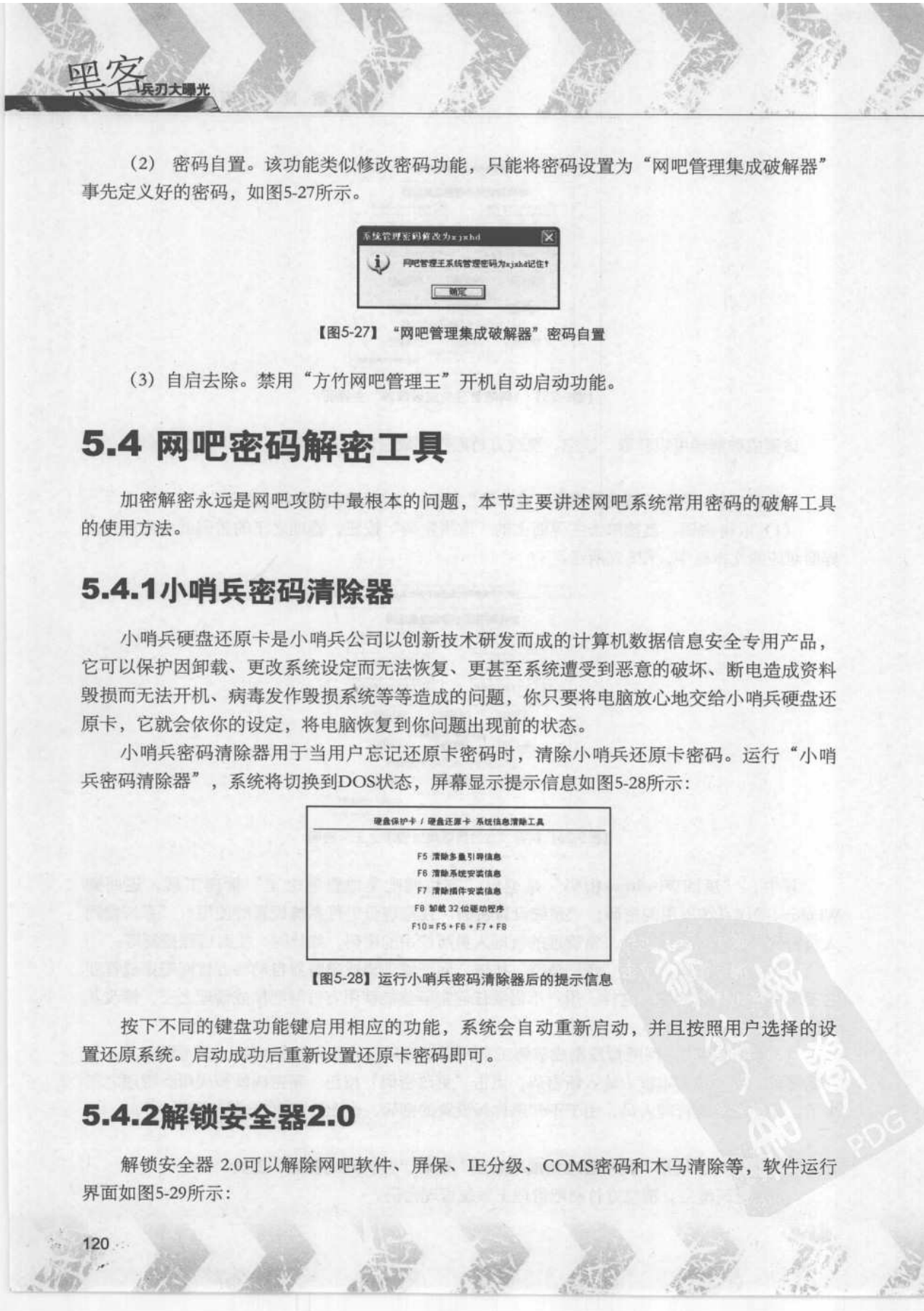
其中，“返回Windows密码”是退出“方竹网吧集成管理之王”管理工具，返回到Windows操作系统所用的密码；“系统设置密码”在管理员进行系统设置时使用；“系统管理人员密码”则是对系统进行日常管理的管理人员所使用的密码，如计时、实时远程控制等。

(2) 清空密码。单击“密码清空”按钮，网吧管理集成破解器自动将方竹网吧集成管理之王所有密码设置为空。这样，用户不需要任何密码就能使用方竹网吧集成管理之王，修改其中的设置。

(3) 修改密码。网吧管理集成破解工具并提供给用户修改密码的功能，在主界面上三个“新密码”对应的文本框中输入新密码，点击“更改密码”按钮，新密码就被应用到管理之王中了。即使是系统管理人员，由于不知道你新设置的密码，也无法使用它进行管理。

【案例5-10】使用“网吧管理集成破解器”破解“方竹网吧管理”工具。

(1) 密码清空。清空方竹网吧管理王系统管理密码。



(2) 密码自置。该功能类似修改密码功能，只能将密码设置为“网吧管理集成破解器”事先定义好的密码，如图5-27所示。



【图5-27】“网吧管理集成破解器”密码自置

(3) 自启去除。禁用“方竹网吧管理王”开机自动启动功能。

5.4 网吧密码解密工具

加密解密永远是网吧攻防中最根本的问题，本节主要讲述网吧系统常用密码的破解工具的使用方法。

5.4.1 小哨兵密码清除器

小哨兵硬盘还原卡是小哨兵公司以创新技术研发而成的计算机数据信息安全专用产品，它可以保护因卸载、更改系统设定而无法恢复、更甚至系统遭受到恶意的破坏、断电造成资料毁损而无法开机、病毒发作毁损系统等等造成的问题，你只要将电脑放心地交给小哨兵硬盘还原卡，它就会依你的设定，将电脑恢复到你问题出现前的状态。

小哨兵密码清除器用于当用户忘记还原卡密码时，清除小哨兵还原卡密码。运行“小哨兵密码清除器”，系统将切换到DOS状态，屏幕显示提示信息如图5-28所示：



【图5-28】运行小哨兵密码清除器后的提示信息

按下不同的键盘功能键启用相应的功能，系统会自动重新启动，并且按照用户选择的设置还原系统。启动成功后重新设置还原卡密码即可。

5.4.2 解锁安全器2.0

解锁安全器 2.0可以解除网吧软件、屏保、IE分级、COMS密码和木马清除等，软件运行界面如图5-29所示：

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



系列、将死者病毒、偷QQ密码、狐Q木马、冰河木马、NetSpy、爱虫病毒、Backdoor等木马和病毒。从图5-32种可以看到完整的列表。



【图5-32】解锁安全器清除木马

(4) 除了解锁和木马清除外，“解锁安全器”还可以禁用某些系统功能：如禁止编辑注册表、禁止MS-DOS方式、禁止IE主页修改等。这些限制可以减少病毒、木马或其他恶意程序入侵系统。

选中主界面上各个功能项前面对应的复选框，然后单击“保存设置”按钮即可。但要注意，有些设置需要重新启动计算机才能生效，而“解锁安全器”不会提醒用户重启计算机，建议大家在修改了系统设置之后最好手动重启机器，应用所做的设置修改。

(5) 系统与用户管理：通过“解锁安全器2.0”，用户可以方便地查看和修改某些系统信息和用户信息。选择但选按钮组中的“系统与用户”项，主界面上会显示计算机操作系统版本、计算机名、工作组、使用者名和使用者单位等信息，如图5-33所示。



【图5-33】解锁安全器系统与用户管理

选择“修改系统与用户设置”复选框，可以对系统和用户信息进行编辑，编辑结束后单击“保存修改”按钮保存修改后的系统和用户信息。

5.4.3 BIOS密码探测器

为了保护计算机上用户数据的安全性，操作系统为用户提供了开机时使用的CMOS密码，根据用户设置的不同，可以分为两种情况。

一种是SETUP密码，采用这种方式时，系统可以直接启动，而只是在用户进入BIOS设置时才要求输入密码；另一种是SYSTEM密码，采用这种方式时，无论是直接启动还是进行BIOS设置都要求输入密码。

BIOS密码是用户进入BIOS设置时要求输入的密码。如果忘记了CMOS密码，而你又急需进入BIOS程序进行设置和修改，这时就必须破解CMOS密码。传统的做法是打开机箱，给CMOS电池放电，清除CMOS中的所有内容。虽然现在很多主板提供了CMOS密码清除跳线，用户按照主板说明书的指示，可以清除CMOS密码。但这些方法要求用户必须具有一定的硬件基础知识。

BIOS密码探测器用于破解BIOS密码，使用BIOS密码探测器，即使不知道CMOS电池的用户，也可以很方便地读出系统的CMOS密码。

『案例5-12』使用BIOS密码探测器破解BIOS密码。

BIOS密码探测器运行后界面如图5-34所示：



【图5-34】BIOS密码探测器程序界面

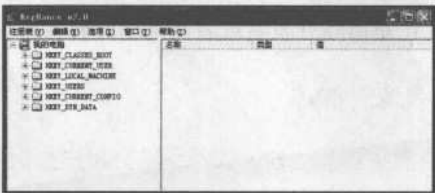
程序运行后单击主界面上的“获取密码”按钮，主界面上对应的文本框中分别会显示系统的BIOS版本信息、BIOS日期、密码和安全选项（如果用户设置了BIOS密码和安全选项），图5-34所示为用户没有设置BIOS密码的情况。

5.4.4注册表解锁器

注册表解锁器用于破解对用户编辑注册表功能的限制，它完全模拟系统注册表编辑器，使用户可以像在本地注册表编辑器中一样在注册表解锁器中对键名、键值等进行编辑。

『案例5-13』使用注册表解锁器编辑注册表。

注册表解锁器文件名和系统注册表编辑器文件名相同，同为regedit.exe，不过两者并非同一文件。双击注册表解锁器的regedit.exe文件，运行结果如图5-35所示。



【图5-35】注册表解锁器程序主界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



与系统注册表编辑器相同，双击主键名可以展开注册表树；右键点击键名可以对主键或键值进行编辑，包括：新建主键、删除、重命名主键，复制主键名、修改键值、搜索以及导入、导出注册表文件等，如图5-35所示。



【图5-36】在“注册表解锁器”中编辑注册表

5.4.5 网上邻居密码破解器

“网上邻居”是局域网用户访问其他工作站的一种途径，用户可以通过它来访问局域网内的共享资源，十分方便。但是如果在打开共享目录时提示需要密码才能访问，用户在不知道密码的情况下，可以使用软件来破解网上邻居密码。

网上邻居密码破解器（PQwak）就是这样一款破解网上邻居密码的工具，可以破解Windows95、Windows98、Windows Me操作系统的共享密码。

【案例5-14】使用“网上邻居密码破解器”破解共享密码。

- (1) 双击运行PQwak.exe文件打开“网上邻居密码破解器”
- (2) 输入需要破解共享密码的主机IP地址和Share（共享文件名），然后单击“Crack”按钮开始破解，很快密码框里就会显示出该共享文件夹的共享密码，还可以看到被破解主机的主机名，显示在“Name”文本框中。

5.5 小结

网游黑客工具和网吧黑客工具相对而言应用都非常简单，基本都是针对软件的漏洞进行工具或者获取密码。因而无论是游戏开发者或者网吧的经营者都应该对这类型的黑客工具引起足够的重视，防患于未然。

第6章 网页黑客工具

网页黑客工具分为网页密码破解工具和网页漏洞扫描工具两种。黑客利用网页漏洞扫描工具扫描网页漏洞，待找出漏洞后，通过网页密码破解工具攻入漏洞并获取网页相关密码，从而攻破目标网站。

在本章中就将为读者介绍一些关于网页的知识。

本章要点

- ◎ 网页密码破解
- ◎ 网页漏洞扫描
- ◎ 猜解数据库
- ◎ 漏洞防范
- ◎ COOKIE欺骗
- ◎ 动网上传利用程序

6.1 网页密码破解工具

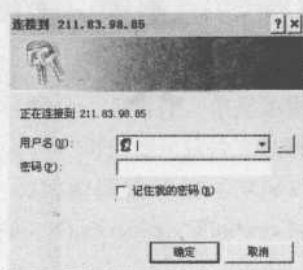
网页黑客工具分为网页密码破解工具和网页漏洞扫描工具两种。黑客利用网页漏洞扫描工具扫描网页漏洞，待找出漏洞后，通过网页密码破解工具攻入漏洞并获取网页相关密码，从而攻破目标网站。

6.1.1 破解原理及方法介绍

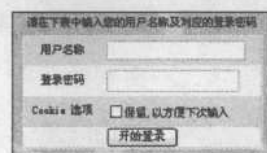
网站的密码验证方式分为两种：弹出式入口密码验证和表单式密码验证。

有些网站（特别是电影、音乐等收费网站）往往在使用IE连接的时候弹出一个对话框，要求输入用户名和密码，如图6-1所示。只有填入IIS中设定的合法账号和口令，才能成功访问。一般称这种密码验证为弹出式入口密码验证。

许多动态网站都采用填写并提交表单的形式登录。例如图6-2是某个网站的邮箱登录表单。在表单中填入正确的用户名和密码就可以登录。这种密码验证称为表单密码验证。



【图6-1】IE弹出网页认证对话框



【图6-2】通过填写表单认证用户信息

下面我们来具体学习几款网页密码破解工具的使用。这些工具要么针对弹出式入口密码验证，要么针对表单式密码验证。通过对这些破解工具的学习，我们会对网页密码破解的原理有更深刻的认识

6.1.2 流光

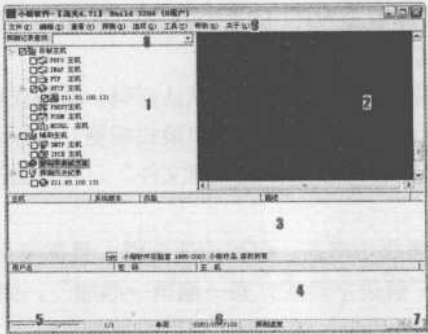
“流光”是一款著名的高集成度网站扫描和网页密码破解工具，具有多线程检测、线程超时处理、用户流模式、163/169双通、多字典同时检测等特点。流光可用来破解网页弹出式入口验证密码。

【案例6-1】使用流光进行HTTP扫描破解网页密码

(1) 运行流光程序，弹出主界面，功能区域主要分为四个部分，如图6-3所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 6 章 网页黑客工具



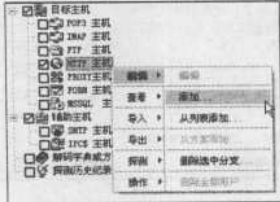
【图6-3】流光程序运行主界面

图6-1所示窗口中各标记部分功能如下表：

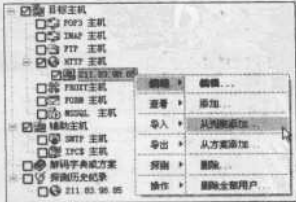
流光各标记部分功能表	
标记	功能
1	暴力破解的设置区域，这个区域主要用于设置暴力破解和其他相关的辅助功能。
2	控制台输出，用于查看当前工作的状态，包括扫描和暴力破解等。
3	扫描出来的典型漏洞列表，在这个列表中大多数情况都可以直接点击，对漏洞加以进一步的验证。
4	扫描或者暴力破解成功的用户账号。
5	扫描和暴力破解的速度控制（通过设置TCP的超时时间来实现）。
6	扫描和暴力破解时的状态显示，包括并发的线程数目和扫描速度等。
7	中止按钮，可以中止暴力破解和扫描（IPC的暴力破解除外）。
8	探测记录查找工具。
9	程序主界面菜单。

(2) 流光的HTTP扫描功能能够快速扫描IIS中设定的非匿名访问账号的用户名和密码，以破解弹出式入口验证。在暴力破解的设置区域选择“HTTP主机”，单击鼠标右键，选择“编辑→添加”，如图6-4所示，在弹出的对话框中添加扫描的目标主机。这里我们添加IP地址为“211.83.98.85”的主机。

(3) 为了破解网页用户名，需要为流光加入用户名的列表文件。在刚才添加的IP为“211.83.98.85”的机器上单击鼠标右键，选择“编辑”→“从列表添加”，如图6-5所示，在弹出的对话框中选择“Name.dic”这个流光自带的字典文件。



【图6-4】流光中添加扫描的HTTP主机



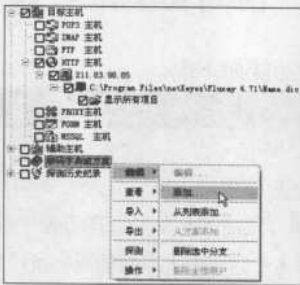
【图6-5】流光中添加扫描主机的用户名列表文件



(4) 有了用户名，就可以着手对HTTP服务器进行探测了。流光的探测包括“简单模式探测”和“标准模式探测”两种。

● “简单模式探测”仅使用“123456”作为默认密码，探测成功率低，但速度非常快，适用于探测设置了简单密码目标机器的情况。“简单模式探测”的探测密码可以手动添加，方法是点击“工具→模式文件设定→简单模式探测设置文件”，在弹出的文本文件中每一行输入一个密码就可以了。

● “标准模式探测”探测成功率高，但探测速度慢，且需要用户口令字典的支持。添加用户口令字典的方法是点击“解码字典或方案→编辑→添加”，如图6-6所示，并选择一个口令字典文件。本例选择“Password.dic”这个流光自带的字典文件。



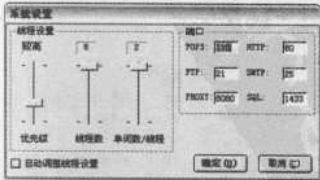
【图6-6】流光中添加用户口令字典

(5) 首先使用“简单模式探测”来探测目标站点的密码。单击“探测→简单模式探测”，就开始探测HTTP主机。如果探测到合法用户名和密码，将弹出“探测结果”窗口，并在简单探测结束后启用多线程模式进一步验证。探测过程如图6-7所示。

注意：流光的探测可以采用多线程模式进行。但HTTP探测必须从单线程模式启动，否则将提示“在NTLM/Negotiate方式中，请将线程数目设置为1”的错误。点击“选项→系统设置”，在弹出的“系统设置”窗口中设置探测线程数，如图6-8所示。要设置为单线程模式，直接将“线程数”滚动条拖动到上端即可。



【图6-7】使用流光的HTTP“简单模式探测”



【图6-8】流光中设置探测线程数

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(6) 探测结束后，流光在“本次探测用户”窗口中显示探测到的用户名和密码，如图6-9所示。



【图6-9】流光报告探测结果

(7) 当流光询问是否生成HTTP方式的分析报告时，选择“是”，即打开一个IE窗口，并在这个窗口中显示全面的“入侵检测报告”，如图6-10所示。报告包括本次探测的时间、范围、结果等相关信息，清晰地再现了整个探测过程。



【图6-10】流光生成分析报表

使用“标准模式探测”的方式和使用“简单探测模式”类似，读者不妨亲自尝试一下，本节不再赘述。

【案例6-2】使用流光对目标机器进行全面探测。

进行HTTP探测仅是流光探测功能的很小一部分。流光还可以进行POP3、IMAP、FTP、MSSQL等许多探测。由于不是本章的重点，这里只对非HTTP的探测进行简要介绍。

(1) 如果要对目标机器进行全面探测，单独设置每一种探测项目比较麻烦，可以利用流光专门提供的探测向导功能来进行设置。单击“文件”→“高级扫描向导”，弹出“设置”窗口如图6-11所示。这个“设置”窗口可以辅助我们一步步对扫描选项进行设置。

(2) 在图6-11的第一个设置窗口中，输入探测的地址范围，起始地址和结束地址都是“211.83.98.85”，单击“全选”按钮，选择探测所有协议。

(3) 一直单击“下一步”按钮，默认流光的全部设置，最后选择“猜解用户名字典”和“猜解密码字典”的路径，并点击“完成”结束设置，如图6-12所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



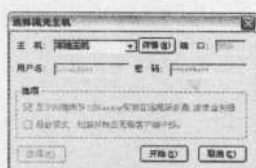
【图6-11】流光的高级扫描向导1



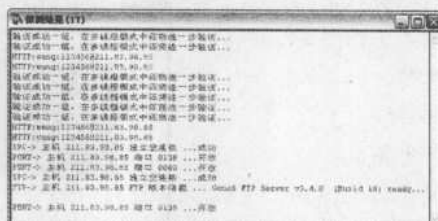
【图6-12】流光的高级扫描向导2

(4) 结束设置后,流光弹出“选择流光主机”窗口,如图6-13所示。这里默认接受“本地主机”的默认设置,单击“开始”按钮就可以了。

(5) 流光开始对目标主机全面扫描。如果扫描到有价值的信息,会弹出“探测结果”窗口,并将信息显示在这个窗口中,如图6-14所示。如果同意生成报表,流光会将本次扫描的详细结果生成HTML报表并打开IE窗口显示。



【图6-13】流光的选择流光主机窗口



【图6-14】流光显示探测结果

进行攻击之前，首先需要对流扫扫描到的目标机器各种漏洞有所了解。例如，21端口开放，让人想到wu_ftp溢出攻击；53端口开放，可能存在远程溢出漏洞；3389端口开放则可能利用输入法漏洞攻入系统；137-139端口开放意味着可以通过共享资源漏洞入侵；80端口开放可以尝试执行IIS的“Remote Execute A”远程命令获取系统权限。

黑客利用流光扫描和攻击服务器的一般攻击流程是：

- (1) 确定攻击目标;
- (2) 通过流光软件搜集目标的相关资料和信息;
- (3) 根据获得的信息尝试攻击目标机器, 或潜入机器的操作系统;
- (4) 利用权限提升手段使自己获得系统最高权限, 完成攻击;
- (5) 清理目标机器系统日志, 并为目标机器植入木马后门, 以备后用。

而黑客通过流光获取系统信息后,攻击目标机器的手段通常有:

- (1) URL攻击, 比如URL的Unicode漏洞攻击。通常在IE地址栏通过提交修改的URL地址, 非法登录或者非法浏览;
- (2) 暴力破解, 这种方法比较费时, 但也有一定的技巧可寻, 比如用finger探测后的用户列表进行二次探测。
- (3) 系统相关服务攻击, 比如终端输入法漏洞攻击、Frontpage扩展攻击、服务器缓冲区

溢出攻击等。

下面通过一个实例来演示如何利用流光的扫描结果对网站进行Unicode攻击。



在计算机中英文字母用单字节表示，而中文文字需要用双字节来表示。对于不同字符系统而言，要解决中英文字符混合使用的情况，必须经过字符码转换，非常麻烦。为解决这个问题，Apple、Microsoft、IBM、Borland等很多公司联合起来制订了一套适用于全世界所有国家的字符码，称为Unicode。

Unicode攻击指通过系统Unicode漏洞入侵目标机算计的攻击。Unicode漏洞的一个典型例子是对下面的一种编码方式：

`%c1%1c`

IIS却根据HTML编码规则理解为：

$(0xc1 - 0xc0) * 0x40 + 0x1c = 0x5c = '/'$ 。

又如对

`%c0%2f`

IIS却理解为：

$(0xc0 - 0xc0) * 0x40 + 0x2f = 0x2f = '\'$

通过小小的“/”和“\”，我们就可以构造特殊URL来深入到系统的根目录下。

【案例6-3】分析流光扫描结果，进行Unicode攻击实例。

(1) 首先使用流光扫描目标机器是否存在IIS的Unicode漏洞。在流光主界面上单击“文件”→“高级扫描向导”，在“检测项目”中选择“IIS”，并单击“下一步”。在弹出的“IIS”对话框中，选择“Unicode编码漏洞”，单击“下一步”完成，如图6-15所示。



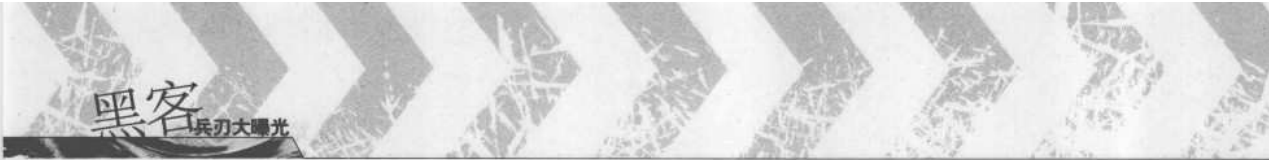
【图6-15】配置流光扫描Unicode编码漏洞

(2) 扫描机器“211.83.98.85”存在的Unicode漏洞后，打开IE，并在地址栏输入下面的URL：

`http://211.83.98.85/..%c1%1c../windows/system32/cmd.exe?/c+dir%20c:\`

其中“`..%c1%1c`”表示退到上级目录，“`%20`”表示空格，这样就利用IIS的帮助执行了

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Windows系统目录下的cmd.exe命令程序，并利用cmd.exe的参数在命令行中执行了dir（列举目录）命令，如图6-16所示。只需要将URL中的“dir”改为其他相关命令，就可自由控制“211.83.98.85”这台机器做想做的任何事情。



【图6-16】利用IIS的Unicode漏洞对目标机器进行攻击

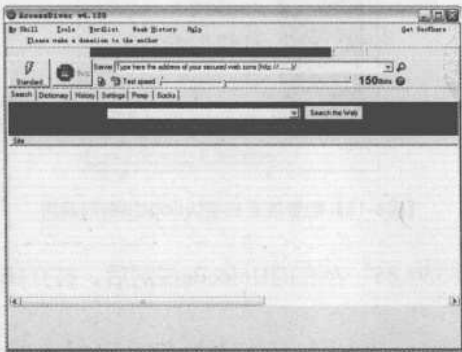
6.1.3 AccessDiver

AccessDiver是国外最有名的检测网站安全漏洞的工具，同时也是目前最好的网站破解工具之一。它能够通过不同代理服务器多线程检测和破解弹出式入口验证加密的网站，并以攻击的方式查验网站保密系统的安全系数，对网站的安全性进行全方位测试。

AccessDiver的功能比较全面，而暴力破解是它最基本、最常用的功能，原理是使用大量代理做掩护，对已有的用户名/密码组合进行逐个验证，从中找到有效的组合。除此之外，AccessDiver的代理分析功能和字典制作功能也比较实用。AccessDiver还有很多有特色的功能，比如debug、exploit、Auto-Pilot等。

「案例6-4」使用AccessDiver破解网站。

运行AccessDiver，弹出主界面，如图6-17所示：

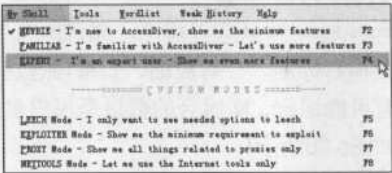


【图6-17】AccessDiver软件的运行主界面

AccessDiver的基本使用。

1.切换用户模式

单击主界面菜单上的“My Skill”→“Expert - I’ m an expert user - Show me even more features”，将AccessDiver切换到专家模式。在专家模式中，AccessDiver的全部功能得以打开，如图6-18所示。



【图6-18】 AccessDiver软件切换用户模式

2.配置系统选项

单击“Setting”标签进行系统配置。“Settings”下有七个不同的选项卡标签。

(1) Access标签

“Analysis accuracy”框中的两项，通常情况下都勾选。

“Temporisation”延迟选项框一般不需要勾选。

“Disable fake login detection during a [Standard] security test”指在标准模式（弹出式入口）测试时禁用fake探测功能。这个选项如果勾选，则探测时可能会出现很多假密码。

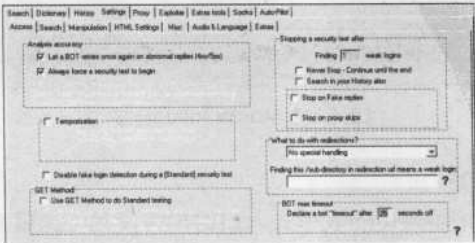
“GET Method”框只有“Use GET Method to do Standard testing”选项。这个选项使用GET方法进行标准模式（弹出式入口）测试，一般不勾选。

“Stop a security test after”框可以选择停止安全测试的方式，例如“Never Stop—Continue until the end”指一直跑完整个字典，“Stop on Fake replies”指出现fake假密码时停止，“Stop on proxy skips”指出现代理跳过时停止。都不勾选。

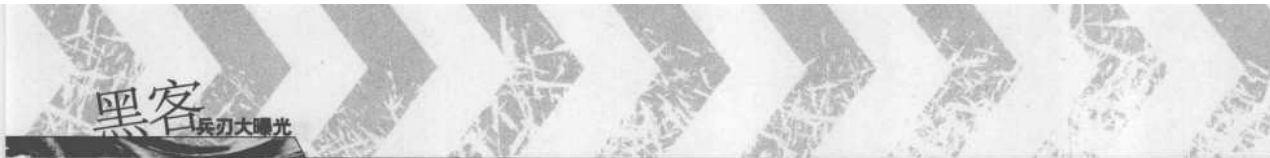
“What to do with redirections”框中，一般选择“No Special Handling”。

“BOT max timeout”框中，可以设置线程超时的最大时间。如果网络状况不好或代理速度较慢，可以适当增大框中的数字。

Access标签下的推荐设置如图6-19所示。



【图6-19】 Access标签下的推荐设置



(2) Search标签

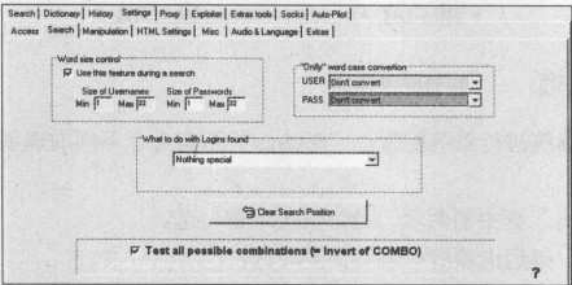
“Word size control”框中，勾选“Use this feature during a search”可以对用户名和密码的长度加以限制。限制用户名和密码的长度可以缩短验证时间，并减少使用代理时的损失。

“Only word case conversion”设置用户名和密码的格式，如“全部大写”、“全部小写”或“首字大写”等。

“What to do with logins found”，直接选择“Nothing Special”。

“Test all possible combinations(=invert of COMBO)”测试所有可能的用户名/密码组合。默认状态下AccessDiver字典中用户名和密码是一一对应的。如果勾选这个功能，AccessDiver将会尝试当前字典中用户名和密码的所有可能组合，而组合的数量是用户名数量和密码数量的乘积。

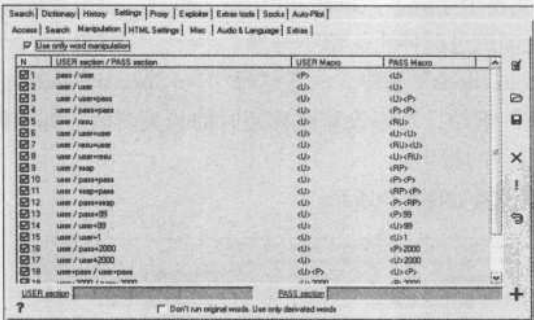
Search标签下的推荐设置如图6-20所示：



【图6-20】Search标签下的推荐设置

(3) Manipulation标签

勾选“Use only word manipulation”，可以对字典进行一些特殊处理，比如给每个用户名或密码加上统一后缀，如图6-21所示。这里不勾选“Use only word manipulation”。



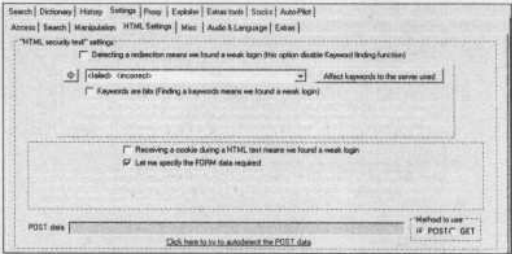
【图6-21】Manipulation标签

(4) HTML Settings标签

HTML Settings标签用来填写form表单式入口的相关设置，这里需要勾选“Let me specify the FROM data required”。

HTML Settings标签下的推荐设置如图6-22所示：

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图6-22】HTML Settings标签下的推荐设置

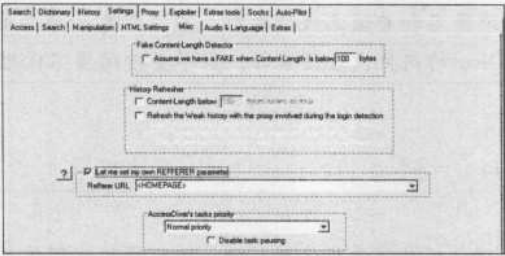
(5) Misc标签

“Fake Content-Length Detector” 框用来勾选并且设置低于多少字节的“content-length”为fake假密码。这个选项可以根据目标返回的fake信息决定是否勾选。

“History Refresher” 框是关于历史记录的再次验证设置。

“AccessDiver's tasks priority” 设置AccessDiver的运行进程优先级为正常模式或者低优先级模式。如果AccessDiver运行时占用大量系统资源而导致系统失去响应，应设置为“Lower priority”低优先级模式。

Misc标签下的推荐设置如图6-23所示：



【图6-23】Misc标签下的推荐设置

(6) Audio & Language标签

该标签下的设置和我们的探测无关，可以忽略。

(7) Extras标签

“Auto-Clipboard” 下拉框中，可以选择将Windows剪贴板中的内容自动复制到一些AccessDiver的分析工具中。

“Duplicate Remover” 框用于选择是否测试大小写不同而用户名/密码相同组合。一般不选这个功能。

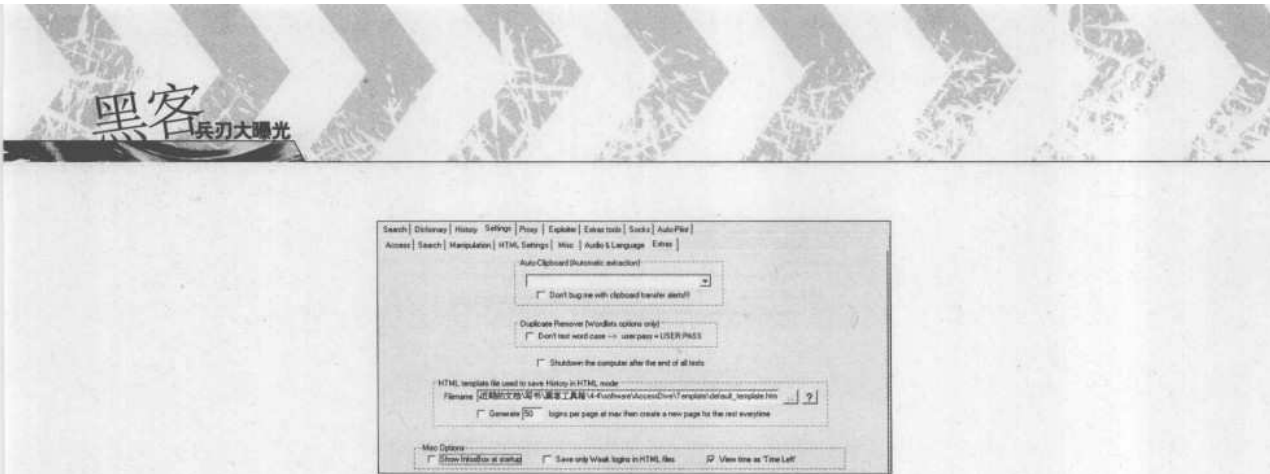
“Shutdown the computer after the end of all tests” 选择是否在完成所有验证后自动关闭计算机。

“HTML template file used to save History in HTML mode” 用于选择记录日志的HTML模板。

“Misc Options” 框内，不选“Show InfosBox at startup”以去掉AccessDiver的启动画面。

Extras标签下的推荐设置如图6-24所示：

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图6-24】Extras标签下的推荐设置

3. 设置用户代理

通过HTTP代理服务器（HTTP Proxy Server）的代理来访问网站。代理服务器代理客户端访问目标网站，并将访问的数据回传给客户端。

设置用户代理在AccessDiver中非常重要。目前绝大部分网站的密码验证系统都有IP监测系统，如果发现相同IP尝试非法登录次数过多，会将该IP列入黑名单，使之无法继续进行连接。因此，如果使用固定IP来进行网页密码探测，很快就会被禁止掉。使用频繁变换的代理来帮助进行密码验证是解决这个问题的有效办法。

注意：HTTP代理分为匿名和非匿名代理两种。匿名代理一般不会向目标网站报告客户的真实IP，因此进行AccessDiver的用户代理设置时，应尽量使用匿名代理。



AccessDiver的代理分析功能分析速度较快，但获得的代理信息较少。例如，它无法获知代理服务器所在的国家，也不能分析代理是否支持SSL。要获得关于代理服务器的更多信息，可以选用专门的代理分析工具，如ProxyChecker、ProxyHunter、代理之狐等。

单击“Proxy”标签进行用户代理设置。“Proxy”下有4个不同的选项卡标签。

(1) My LIST标签

勾选“Rotate proxies”，“[] logins before swapping”一般在1~5之间，即每个代理只验证一组密码就立刻更换其它代理，这就使得目标网站不容易发现黑客的探测。

“Proxy skipping”前三项分别表示在出现“errors(4xx/5xx)”，“fake replies”和“redirections”的情况下更换代理，一般都选择。第四项是破解HTML入口时的一个选项。最后一个选项“Retry the user:pass again after skipping”指出现proxy skipping以后更换代理重新验证这组密码，一般也选择。

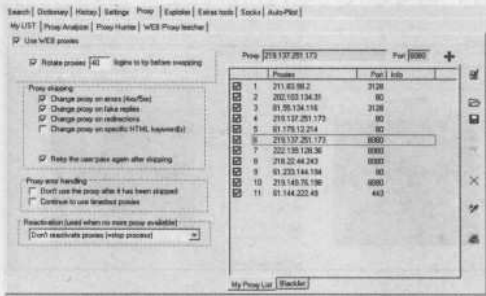
“在Proxy error handling”框中“Don't use the proxy after it has been skipped”指出现“proxy skipping”后不再使用这个代理，“Continue to use timeout proxies”指继续使用超时代理，一般

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

不需要勾选。

在“Reactivation (used when no more proxy available)”下拉框选择“don't reactivate proxies(=stop process)”，这样失效的代理不会被重复使用，当没有可用代理时验证就自动终止。

My LIST标签下的推荐设置如图6-25所示：



【图6-25】My LIST标签下的推荐设置

(2) Proxy Analyzer标签

在进行代理分析之前，为了保证代理的可用性，可以用Proxy Analyzer来验证匿名代理的可用性。

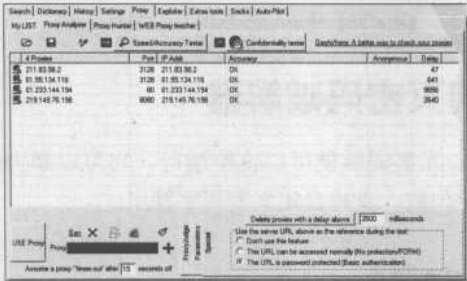
在Proxy Analyzer标签下，点击右下方的“Proxyjudge”标签，显示proxyjudge列表框。在列表框中单击鼠标右键，选择“Verify all scripts”校验所有代理脚本。校验完毕后，从列表框中勾选1~3个速度最快的有效脚本，以便使用它们来检验代理的匿名性。

注意：Proxyjudge校验要经常进行，以保证当前使用的脚本不但有效而且保持速度最快。

接着单击右下方的“Parameters”标签，选择“Auto-deletion of bad proxies after a test completion”和“Auto-delete proxies based on their proxy level criteria(See proxyjudge settings)”。

单击右下方的“Special”标签，选择“The URL is password protected(Basic authentication)”如图6-26所示。

单击“Open”图标，打开一组代理文本文件（目前许多网站都有免费代理列表，直接将代理列表保存为“1.2.3.4:8080”列表的文本文件即可），并点击“Speed/Accuracy Tester”，AccessDiver启动代理验证过程。验证完毕之后，选中全部代理，另存为新的代理文件即可。



【图6-26】Proxy Analyzer标签下的推荐设置

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



4.设置字典

单击“Dictionary”标签进行用户代理设置。“Dictionary”下有四个不同的选项卡标签。

单击“Currently used”标签，并点击“导入”图标导入字典文件。字典文件可以使用AccessDiver事先准备的文件，也可以使用通过用户自定义手段定义的新文件，如图6-27所示。



【图6-27】AccessDiver软件设置字典

5.破解网页密码

通过上面三个步骤对AccessDiver进行正确设置后，就可以轻松破解网页密码了。

将目标网页的URL地址复制到AccessDiver的“Server”框中，如图6-26中的1处，点击左上角的Standard按钮，如图6-28的中两处，AccessDiver立即启动破解过程。在破解过程中可以随时通过“Test speed”拖动条（位于“Server”框下面）动态改变线程数“Bots”来调整验证速度。破解了网页“http://211.83.98.85”的入口用户名是“www”，密码是“passwww”。



【图6-28】使用AccessDiver破解网页密码

6.1.4黑雨——网页密码破解器

黑雨是一款国产软件，无需安装便可以运行。它可以暴力破解网页表单密码，支持多线程模式、指定密码起止位数、支持自定义密码字符串。

【案例6-3】使用黑雨破解网页。

(1) 运行黑雨，弹出主界面，如图6-29所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 6 章 网页黑客工具

(2) 以破解表单密码验证的网页http://211.83.98.85/office，如图6-30所示，来学习黑雨软件的使用。



【图6-29】黑雨的运行主界面



【图6-30】一个典型的表单密码验证页面

(3) 获取网页信息

在页面上单击鼠标右键，选择“查看源文件”，在源文件代码中找到“<form>”标签到“</form>”标签之间的代码，即表单登录框的HTML代码，如图6-31所示。



【图6-31】一个典型表单密码验证页面的源文件代码

“<form>”标签中的“method=“post””表示HTTP请求方法为“post”，“action=checklogin.asp”是表单的发送地址。

“<input>”标签中的“login”和“password”表示表单发送的数据。

(4) 配置黑雨参数

单击“设置”标签，对“密码串”/“用户串”、密码起始和结束位数、最大线程数等进行配置。一般网页表单密码均由小写字母和数字组成，所以一般“密码串”选择数字和小写字母，并将最大线程数设为4，如图6-32所示。



【图6-32】黑雨的基本配置

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



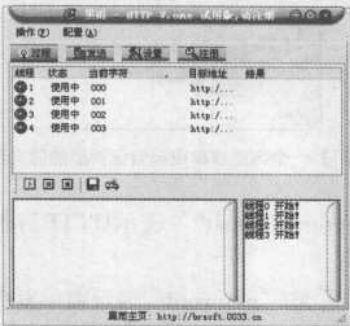
(5) 接着单击“发送”标签，根据前面第一步中获得的参数，填写“发送地址”为“http://211.83.98.85/office/checklogin.asp”，选择“Http请求”方法为“Post”，发送数据为“login=#username# password=#password#”，如图6-33所示。



【图6-33】黑雨的数据发送参数

(6) 利用黑雨破解表单

配置完成之后，单击“过程”标签，并点击开始图标进行破解，如图6-34所示。一段时间后，破解成功，黑雨会将找到的用户名和密码显示在左下角文本框中。



【图6-34】用黑雨进行网页密码破解

6.2 网页漏洞扫描工具

黑客攻击和破解网页的第一步工作，往往是利用网页漏洞扫描工具对目标网站进行扫描，找出漏洞，为后续工作做好准备。本节介绍两种黑客常用的网页漏洞扫描工具。

6.2.1 网页漏洞简单介绍

我们知道，现在的网站特别是稍微大一点的网站，一般都采用ASP、PHP或者JSP等脚本语言来连接数据库，取得数据库里面的数据生成动态网页，这样，当一个网站完全建立以后，程序就会很多，特别是网页设计的特殊性，服务器与用户的交互程序特别多，所以，如果程序员

不是很有经验或者没有强烈的安全意识，程序的漏洞就会很多，给网站带来不可估量的安全隐患。这些程序漏洞，一定程度上，可能比网站服务器的漏洞更加严重，因为这些漏洞防火墙或者入侵检测系统根本无法防止。

一、编程漏洞的形成

编程漏洞怎么形成的呢？需要对网页编程有比较全面的认识才可以理解。首先，我们来看看网页编程的特点。

1. 网页编程交互性强

之所以采用各种语言来设计网站而不直接采用HTML，目的就是为了更好地管理网站资源，增加网站与浏览者之间的交互。所以，在网站设计的时候，一些常见的交互编程是少不了的，比如留言板、BBS论坛，聊天室等，这些程序最大的共同点就是用户输入很多资料，通过这些资料与其他浏览者交流或者与网站管理者交流。而交互的特点，正式漏洞形成的一大原因，因为用户输入信息是不可预测的，如果程序没有考虑到或者考虑不全面一些安全问题，用户输入就有可能成为攻击事件，不管有意还是无意。

2. 网页编程字符处理特别多

上面我们谈到，交互其实就是信息的流通。所以，这些信息的处理就是大问题，怎样严格控制用户输入信息的内容、信息格式、信息长度都是编程需要考虑的问题。

3. 网页编程涉及安全最里层

众所周知，网页编程直接和服务器打交道，这些程序都是直接和网站目录、网站数据库设置网站设置、系统设置相关，通过这些程序，可以访问网站目录、设置等几乎所有服务器内容。仔细想，这些程序其实都是很有潜在安全问题的，因为它们太敏感了。所以，如果程序设计有漏洞，几乎就等于网站有漏洞，甚至完全开放。

4. 网页编程整体人员基础较差

网页编程人员的技术素质，这个问题可能关注得比较少。在部分传统程序员眼中，网页程序设计其实不能称为程序员，他们认为网页程序设计，只需要美工好就可以了，完全没有技巧可言，不叫真正的编程。之所以形成这种观点，有几个原因。一是网页编程相对比较简单，变化较少，基本上，网页编程可以很简单地概括出几个类型：留言板、论坛、聊天室、邮件列表、新闻发布、软件下载等，而这些类型的编程，大部分都有模式可循，和传统编程相比，的确比较简单，任意掌握；二是网页编程人员大部分半路出家，专业的程序员相对较少，编程的系统训练较少，可能编程的基础也比较弱，所以，编程方面允许一些缺陷存在；三是部分网站直接下载网上免费程序来建立网站，这些程序的健壮性、安全性都没有严格考虑，如果网站采用者不自己修改这些程序而直接照搬的话，很可能存在严重安全问题。

二、编程漏洞的类型

网页编程相对比较简单，漏洞的形成实例虽然很多，但是，都有一些内在的共同点可以寻找，这里归纳出一些共同的特点，供我们参考。

1. 用户输入验证不全面

在网站编程而言，有一个规则需要牢记，那就是对于用户和用户的输入，都必须抱怀疑态

度，不能完全信任。对于用户的输入，不能简单地直接采用，必须经过严格验证，确定用户的输入是否符合输入规则才可以实现录入数据库。总结用户输入验证，应该包括以下几个方面。

(1) 输入信息长度验证

这一点可能我们注意得比较少，因为往往认为一般用户不会故意将输入过分拉长，即使有一些用户可能捣乱，但是，在这一点上可能没有危害。其实，如果不进行输入验证，危害可能会相当大，为什么？如果用户输入的信息达到几个兆，而程序又没有验证长度，危害就有：
a、程序验证出错；b、变量占用大量内存，出现内存溢出，甚至可能使服务器服务停止甚至关机。这样的危害多大！

(2) 输入信息敏感字符检查

平时在设计程序的时候，主要关注的是一些JavaScript的敏感字符，比如在设计留言板的时候，会将“<”等符号的信息去除，以免用户留下页面炸弹。是否这些就已经足够了呢？还远远不够。以下几个方面我们需要特别注意。

a. 留言板内容信息的过滤

这一点上面已经提到，平时也使用较多。

b. 用户名信息的过滤

这一点其实我们常常验证，但是，用户名的验证往往只是验证长度，没有验证JavaScript或者HTML的标记，这样就容易形成漏洞。比如用户在用户名填入“<h1>黑</h1>”，一般的用户名验证都可以通过，但是，显示在网页中却是很不美观的。这个输入没有破坏，但是，如果用户名验证不严，没有长度限制，后果怎样呢？这样的漏洞在网上很多！

c. E-mail信息的验证

验证E-mail信息，我们往往也只是是否含有“@”符号，其他没有限制，容易形成两个漏洞：一是输入信息过长的内存溢出漏洞；二是含有JavaScript等字符信息，造成显示用户E-mail的时候形成页面炸弹等。

d. 搜索信息的验证

搜索信息也要验证吗？当然要验证！尽管搜索信息不会直接保存到网站服务器，但是，搜索信息确与数据库或者服务器所有文件密切相关，如果搜索信息有问题，很容易暴露一些本来不应该暴露的数据库信息或者文件信息。而且，如果使用者对程序比较了解，那么这种情况就更加需要注意，使用者可能会利用对于程序的了解，来设计一些很特别的搜索信息，而这些搜索信息其实是会检索其他不应该检索的数据库表的，比如用户账号密码表等。因此，那些从网上下载回来的程序，一般不适宜于直接使用，因为它们的源代码都可以被所有人知道，安全性当然不是很好。在这种情况下，我们一般验证一些常见的用于数据库操作的语句，必须搜索信息是否含有“Select”等，这样来限制使用者输入，避免信息的泄露。

2. 页面行为方式缺乏逻辑

可能这一点看起来很不好理解，页面行为方式是什么呢？举例说明。在一般的网站中，注册新用户的时候，会首先要求用户输入自己需要注册的账号信息，以此来验证该账号是否已经存在，确保用户的单一性。这样的要求，网站编程者的考虑很好，例如新浪注册新用户的时候，就是这样要求的。然而，如果编程不谨慎，容易造成一个很大的漏洞，致使用户信息流

失、出错等情况的发生。这种情况怎样产生的呢？其实很简单，这些页面在编程的时候，认为如果用户的注册信息通过了刚才提到的“检测时候存在该账号”，那么，程序就认为这个账号一定不存在，可以注册，在真正的注册页面中，直接使用“Insert Into”语句将注册信息插入用户数据库就可以了。仔细看看这样的注册过程，发现有一个大的漏洞，那就是，将注册信息插入数据库之前，并没有再一次检查这个用户是否存在，而是很简单的信任前一个检测页面传来的账号信息。我们知道，HTML文件是可以阅读源代码并且也可以直接保存的，如果用户将注册通过的页面保存并且将上面的账号信息修改为一个已经存在的账号，由于程序认为该账号已经通过检测，于是，直接将该账号插入数据库，结果，原来拥有该账号的用户就被删除或者信息被修改了。而如果这个账号刚好是一个管理员账号，结果会怎样呢？

可能我们认为以上的情况很简单，的确简单，但是这种方式编程的程序员却很多，随便在网上找找，可以找到很多这种方式编程的源代码和已经采用的程序。

以上就是页面行为方式缺乏逻辑的典型举例，还有没有其他的举例呢？大家都很熟悉的一个例子：在电子商务初期，一些电子商务网站的程序很多存在这样的漏洞，用户可以随意定义自己购买商品的价格！其实也就是这个原因造成的。

3. 编程方式不成熟

很多时候，制作者可能根本没有意识到一些漏洞的产生，这时候，不是没有注意安全问题，而是因为缺少经验。这种情况下，制作者就需要多了解一些网络攻击者的进攻方式，以此来修改程序，加固网络、程序安全。我们已经知道的一些漏洞就是这种情况产生的。在一些账号密码验证中，万能密码就是这样产生的，在下面的例子中会作详细介绍。

4. 没有基于内容的检测

上面第一条提到检测的漏洞，我们专门提出基于内容的检测。前面多是技术上的考虑，这里，确实基于国家法律法规的考虑。一个网站的设计完成，除了技术的完善以外，还需要这个网站在国家法律法规允许范围内发布信息，不能随意让自己的网站成为一些别用心的人发布不法信息的平台。所以，有必要对所有用户输入而且有可能显示给其他用户的信息进行内容检测，一般有几类：

- (1) 不文明语句的检测。
- (2) 敏感词汇的检测。
- (3) 关系政治的词汇。
- (4) 国家领导人的姓名，最好过滤。

当然，以上的一些规则，不一定全部要这样，可以根据自己留言、或者论坛的性质来决定哪些需要严格过滤。

三、攻击实例

以下的实例，可能网络上有些网站刚好存在这些问题，希望读者也不要利用这些漏洞做不符合国家法律法规的事情。

1. 万能密码

这个漏洞，一些读者可能已经知道，但是，由于网络上依然很多网站存在这些漏洞，还

是有必要详细、全面了解这个漏洞的形成原因和严重后果。首先来看看漏洞的产生。这个漏洞是因为在程序验证账号密码的时候不严谨造成的。我们在程序设计的时候，常常将账号、密码放在一个叫“User”的数据表中，设置“username”和“password”两个字段，当验证的时候，检查用户的输入是否存在于这个数据表，如果存在，证明这个用户合法；不存在，证明用户不合法。漏洞的出现，就是这个验证代码的编写不严谨造成的，我们来看源代码。

‘连接数据库

```
Set Conn=Server.CreateObject("ADODB.Connection")
Connstr="DBQ="+server.mappath("db\news.mdb")+";DefaultDir=;DRIVER={Microsoft Access
Driver (*.mdb)};DriverId=25;FIL=MS Access;ImplicitCommitSync=Yes;MaxBufferSize=512;
MaxScanRows=8;PageTimeout=5;SafeTransactions=0;Threads=3;UserCommitSync=Yes;"
```

‘打开数据库连接

```
Conn.Open connstr
```

‘数据库选择语句

```
mysql="select * from user where userid=' " &txtuserid&" ' and pwd= ' " &txtpwd&" "
set rs=server.createobject("adodb.recordset")
rs.open mysql,conn,1,1
```

```
if not (rs.eof) then
```

```
rs.close
```

```
conn.close
```

```
response.redirect"ok_login.asp"
```

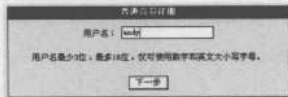
```
end if
```

在以上的代码中，我们看mysql的定义，这里的txtuserid和txtpwd都是直接来自用户的输入，如果用户构造特殊的用户名或者密码，就可以直接让这里的Select条件为“真”，完全不必理会是否有合法账号密码。我们这里不直接给出万能密码，希望有经验的读者仔细分析select语句，找出可能的漏洞。

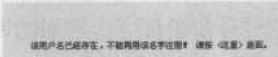
以上漏洞的修改其实很多方法，这里提出几种比较完善的方法供参考。首先，对用户输入的账号、密码进行严格检查，除了二十六字母和十个数字，其他任何字符都是非法的，也就是过滤那些非法的字符，确保用户输入合法。注意，这个过滤要针对用户名和密码进行；二是修改以上的select语句或者下面的if语句，从程序设计角度堵塞漏洞的产生；三是检验用户的输入信息长度，限制输入信息在八个字母内，这样，也能防止漏洞的产生，不过，这个方法不是很好，最好利用第一种方法。

2. 取得别人账号

这个漏洞原因已经在上面分析了，现在来看实例。首先，进入一个注册页面，如图6-35所示，并且随意输入一个账号，出现账号已经存在的信息，如图6-36所示。

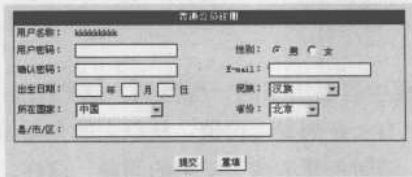


【图6-35】注册页面



【图6-36】账号已经存在提示

怎样取得这个账号的使用权呢？使用另外一个账号注册，如果这个账号不存在，会出现以下的页面，如图6-37所示。



【图6-37】正常注册页面

以上页面，就是正常的注册页面，在“用户名称”后面，会发现需要注册的“kkkkkkkkk”账号，再看看这个页面的源代码，查找这个账号，看这个账号出现在哪些地方，我们只看关键的代码：

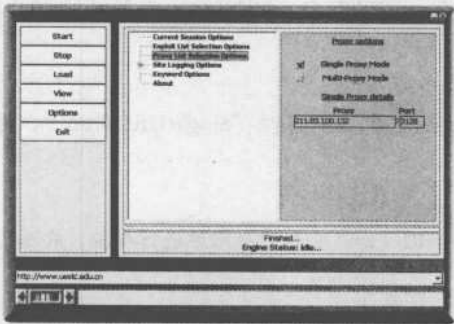
```
<FORM name="form2" action=" ../member/register1.jsp" method=post onsubmit="javascript:
return TestField1()">
<div align="center">
<input type="hidden" name="Step" value="2">
<input type="hidden" name="recName" value=kkkkkkkkk>
<table width="500" border="0" cellspacing="0" cellpadding="2">
<tr bgcolor="#000000">
<td>
<div align="center"><b><font color="#FFFFFF">普通会员注册</font></b></div>
</td>
</tr>
</table>
```

在上面的代码中，发现有两个hidden类型的表单项，第一个是“Step”，第二个是“recName”，从名字可以知道，第一个是注册的步骤，没有意义；第二个是注册的用户名，为什么要使用“hidden”类型表单保存呢？就是为了在以下的正式注册中直接使用这个作为用户名。发现什么没有？可以将这里的注册名修改为我们刚才试验时候使用的注册名“andy”，然后保存为一个HTML文件，再一次打开，填写必要信息提交，结果，取得了该账号的“合法”使用权。在这里需要注意的一点是，在以下语句中：

```
<FORM name="form2" action=" ../member/register1.jsp" method=post onsubmit="javascript:
return TestField1()">
```

如果我们直接保存页面到本机，提交的时候会出错的，因为本机不存在member/register1.

个IP地址频繁连接，会屏蔽这个IP。为了解决这种情况，也可以选择“Multi-Proxy Mode”。



【图6-39】CMXploit的参数配置

(3) 生成Exploit List文件

CMXploit通过Exploit List文件制定要扫描的网页漏洞。必须自己定义一个Exploit List文件。Exploit List文件是一个文本文件，使用Windows自带的记事本程序编辑就可以了。例如图6-40所示就是一个简单的定制文件。

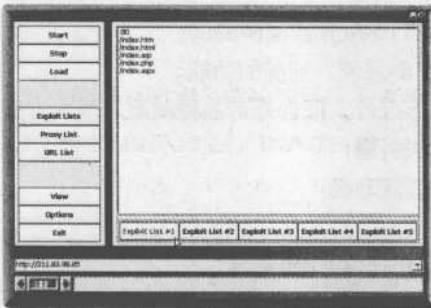
```
#!/usr/bin/perl
use strict;
use warnings;
my $url = "http://211.83.132.132/";
my $path = "/index.htm";
my $exploit = "index.htm";
my $exploit2 = "index.html";
my $exploit3 = "index.asp";
my $exploit4 = "index.php";
my $exploit5 = "index.aspx";
```

【图6-40】定制Exploit List文件

注意：定制Exploit List之前，应该对网站的结构比较熟悉。可以利用IE来浏览网站的各个链接，并记录下这些链接的相对路径。例如浏览网站“http://211.83.98.85/index.htm”，需要记录下“/index.htm”这个相对路径。

(4) 添加Exploit List和目标机器的URL

单击主界面左边的“Load”按钮并点击弹出的“Exploit Lists”按钮，单击右边的“Exploit List #1”按钮，从弹出对话框中选择一个Exploit文件。并在主界面窗口下部添加目标机器的URL地址，如图6-41所示。



【图6-41】添加Exploit List和目标机器的URL

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

黑客
兵刃大曝光

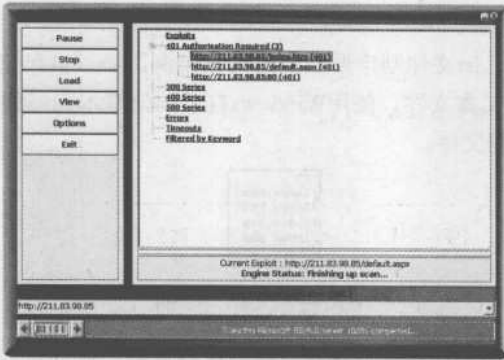
注意：如果使用“Multi-Proxy Mode”多代理模式，必须点击“Proxy List”添加代理列表；如果扫描的网站不止一个，可以点击“URL List”添加网站的URL列表。

(5) 执行网页漏洞扫描进程

单击主界面左边的“Start”按钮，并选择“Single URL Scan”，使CMXploiter开始执行网页漏洞扫描进程。

注意：如果已经添加了“URL List”要对多个网站进行扫描，应选择“Multi-URL Scan”模式。

扫描结果如图6-42所示，根据结果可以判断页面是否加密、是否有错误、是否暂时不能访问等。CMXploiter将不同的错误返回归类并显示。



【图6-42】CMXploiter显示扫描结果

6.2.3 N-Stealth

N-Stealth是N-Stalker公司开发的一款WEB服务器漏洞扫描工具，具有以下特点：

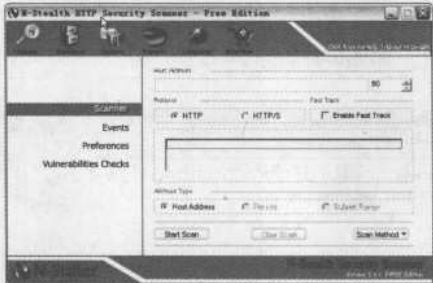
- (1) 能扫描目前几乎所有WEB类型的服务器，包括某些网络设备的WEB控制平台；
- (2) 支持CGI、ColdFusion、ASP、PHP、Lotus Domino、FrontPage等大多数的WEB服务应用程序；
- (3) 能进行超过30000种WEB服务器漏洞测试；
- (4) 带避开IDS（入侵检测系统）捕捉的功能；
- (5) 生成容易解读的图形报告，报告外带各种漏洞的解决方案；
- (6) 带有缓冲区溢出测试引擎；
- (7) 漏洞数据库能进行智能升级。

『案例6-5』使用N-Stealth扫描WEB服务器。

(1) 运行N-Stealth，主界面如图6-43所示。

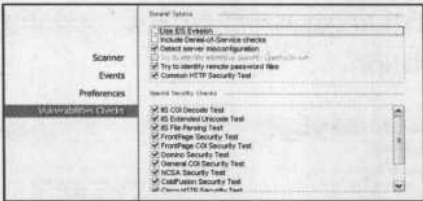
溜客安全网 WwW.176Ku.CoM

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图6-43】N-Stealth的运行主界面

(2) 单击主界面上方的“Scanner”图标，并单击左边的“Vulnerability Checks”，设置各种相关的漏洞扫描测试类型，如图6-44所示。



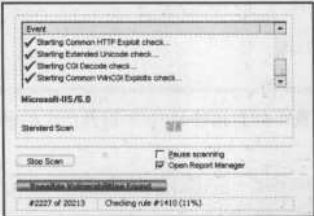
【图6-44】N-Stealth设置漏洞扫描测试类型

(3) 单击左边“Scanner”，在“Host Address”中输入要扫描的目标机器IP地址，如图6-45。单击“Start Scan”开始扫描。



【图6-45】N-Stealth设置目标机器IP地址

(4) 扫描过程如图6-46所示，单击“Stop Scan”按钮可以随时中止扫描。“Vulnerability Checks”中相关测试类型的设置直接影响扫描过程的长短。

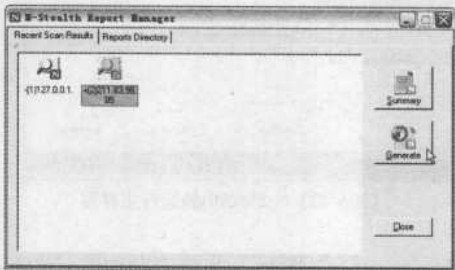


【图6-46】N-Stealth的扫描过程

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

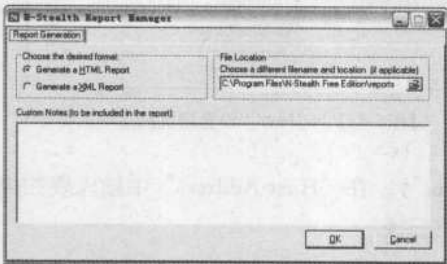


(5) 扫描结束后，N-Stealth会弹出“N-Stealth Report Manager”窗口，选择刚才扫描的机器，并单击“Generate”按钮，如图6-47所示。



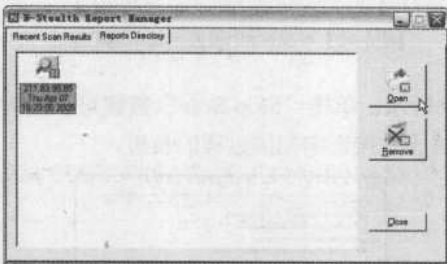
【图6-47】用N-Stealth产生报表

(6) N-Stealth能产生HTML和XML两种形式的报表，本例中选择产生HTML形式的报表，并单击“OK”确认，如图6-48所示。



【图6-48】配置N-Stealth产生HTML形式的报表

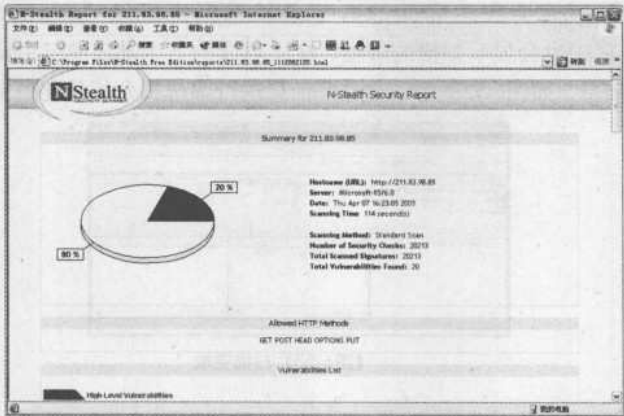
(7) 回到“N-Stealth Report Manager”窗口，选中刚生成的报表，单击“Open”，通过IE浏览器打开报表，如图6-49所示。



【图6-49】用N-Stealth打开产生的报表

(8) “N-Stealth Report Manager”生成的报表内容十分详细，它将漏洞进行分类组织显示，并给出漏洞的解决方案，如图6-50所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



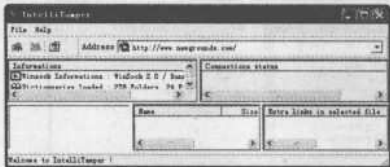
【图6-50】浏览用N-Stealth产生的报表

6.2.4网页扫描和探测——IntelliTammer

有些网站,经常会有一堆跳出来的广告窗口,很讨厌,这个软件是一个容易操作的程序,能告诉你真正躲在网站后面的是什么。

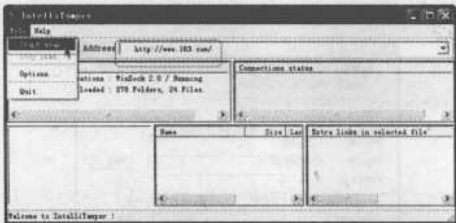
『案例6-6』使用IntelliTammer扫描和探测网页。

(1) 运行IntelliTammer,弹出IntelliTammer的主界面,其菜单栏只有两项,工具栏也比较简洁,如图6-51所示。



【图6-51】IntelliTammer主界面

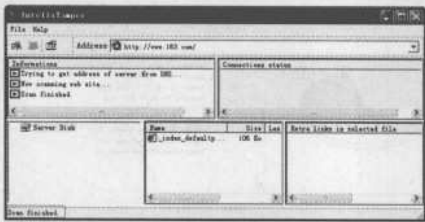
(2) 在工具栏的“Address”栏中输入要扫描的网页的网址,本例中输入http://www.163.com,然后单击菜单栏的“File”,在弹出的下拉菜单中单击“Start scan”开始扫描,如图6-52所示。



【图6-52】开始扫描



(3) 扫描结束后会在主界面的右下角状态栏中显示“Scan finished”字样，在“Informations”栏中也会显示扫描的进度，在主界面的下半部分的三个窗口中会显示当前网页的名称、大小等信息，如图6-53所示。对这些信息进行筛选和分析就能得到想要了解的信息了。



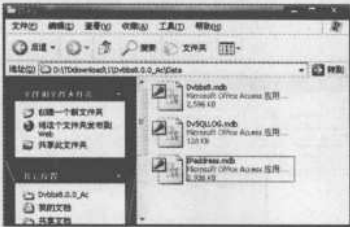
【图6-53】扫描完成

6.3 动网论坛入侵揭密

动网论坛是目前网上最流行的论坛系统之一。漏洞层出不穷，这里我们将详细介绍几种常见的入侵方法。

6.3.1 猜测数据库路径暴力猜解管理员密码

大多数使用动网论坛源代码的管理员，并没有更改数据库的存放位置。数据库的默认存放位置在论坛根目录的data文件夹中，如图6-54所示。



【图6-54】数据库存放地址

如果该动网论坛的版本是7，则数据库的存放名一般是Dvbbs7.mdb或者Dvbbs7.asp，如果该动网论坛的版本是8，则数据库的存放名是Dvbbs8.mdb或者Dvbbs8.asp。在下载工具中，输入下载地址，下载该数据库。比如论坛地址为bbs.forbidden404.com，则下载地址为“http://bbs.forbidden404.com/data/Dvbbs8.mdb”，如图6-55所示。



【图6-55】数据库下载地址猜解

第6章 网页黑客工具

如果猜解正确，则会下载到数据库。如果是ASP结尾的数据库，改为mdb即可。下载到数据库后，运行该数据库，前提条件为必须安装Office Access软件，如图6-56所示。



【图6-56】打开数据库

管理员的用户名和密码就存放在Dv_admin这张数据库表单中，双击该表单，如图6-57所示。



【图6-57】查看管理员用户名和密码

此时可以看见该论坛的管理员只有一个，用户名为admin，密码通过md5方式加密。推荐一个可以在线查看md5密码的网站“<http://www.cmd5.com/default.aspx>”，到该网站上去，输入你在数据库中查到的md5密码，就可以找到正确的密码了，如图6-58所示。

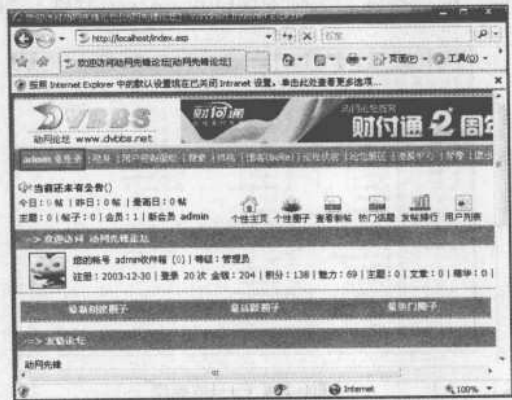


【图6-58】破解md5密码

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



回到该论坛首页，用破解出的用户名和密码登录，登录成功，如图6-59所示。



【图6-59】破解成功

6.3.2 SQL注入攻击方法

随着B/S模式应用的开发，使用这种模式编写应用程序的程序员也越来越多。但是由于这个行业的入门门槛不高，程序员的水平及经验也参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的SQL Injection，即SQL注入。

SQL注入是从正常的WWW端口访问，而且表面看起来跟一般的Web页面访问没什么区别，所以目前市面的防火墙都不会对SQL注入发出警报，如果管理员没查看IIS日志的习惯，可能被入侵很长时间都不会发觉。

但是，SQL注入的手法相当灵活，在注入的时候会碰到很多意外的情况。SQL注入能否成功关键在于能不能根据具体情况进行分析，构造巧妙的SQL语句，从而成功获取想要的数据库。

国内的网站用ASP+Access或SQLServer的占70%以上，PHP+MySQL占20%，其他的不足10%。本文从入门、进阶至高级讲解一下ASP注入的方法及技巧。以一个简单的例子来谈谈SQL注入，给大家一个直观的认识。

【案例6-7】用SQL注入攻击网站。

网站www.19cn.com为例（注：本文发表前已征得该站站长同意，大部分都是真实数据）。在网站首页上，有名为“IE不能打开新窗口的多种解决方法”的链接，地址为：<http://www.19cn.com/showdetail.asp?id=49>，在这个地址后面加上单引号'，服务器会返回下面的错误提示：“Microsoft JET Database Engine 错误 '80040e14' 字符串的语法错误 在查询表达式 'ID=49' 中。/showdetail.asp，行8”。

从这个错误提示能看出下面几点：

- (1) 网站使用的是Access数据库，通过JET引擎连接数据库，而不是通过ODBC；

- (2) 程序没有判断客户端提交的数据是否符合程序要求；
- (3) 该SQL语句所查询的表中有一名为ID的字段。

从上面的例子可以知道，SQL注入的原理，就是从客户端提交特殊的代码，从而收集程序及服务器的信息，获取你想到得到的资料。

必备工具：啊D注入工具、明小子、挖掘鸡
现在简要介绍一下啊D注入工具的使用步骤：

一、查找注入点

先输入一个网址，看看有没有注入的可能性，这里用笔者的机子做测试，地址为http://localhost/sdvod，将该地址复制到地址栏中，点击其地址栏右边的按钮，之后得到有关注入的信息，如图6-60所示。



【图6-60】找到注入信息

其中红色字的链接就是注入点了，双击进入一个新的界面，如图6-61所示。



【图6-61】打开新界面

(1) 检测注入内容。按“检测”按钮即可检测注入内容。接着对表段和字段进行检测，点击“检测表段”将检测出所有的表，如图6-62所示。

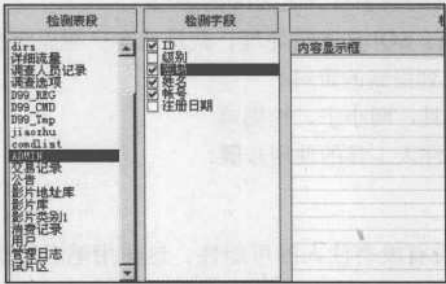
检测表段	检测字段	内容显示框
Reg_Art		
影片类别		
user		
pdf		
dirs		
详细目录		
调查人记录		
调查选项		
D99_ABO		
D99_CBO		
D99_Tap		
jiwozh		
comList		
ADWIT		
交易记录		
公告		
影片地址库		
影片库		
影片类别		

【图6-62】检测所有数据库表

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



(2) 我们再选择Admin表，单击“检测字段”按钮将获得该表的字段信息，如图6-63所示。



【图6-63】检测特定表中的字段

(3) 接下来，选择ID，密码，姓名，账号四个字段来查询，单击“检测内容”获得所选四个字段的内容，如图 6-64所示。

编号	ID	密码	姓名	账号
1	1	eyeyey	油炸鬼	xcyrg
2	9	lanli10	龙李	lanli
3	10	661007	niuguohong	niuniu

【图6-64】检测成功

(4) 由于已经破解到了管理员账号密码等相关信息，接下来的任务就是寻找管理入口，用所得到的账号密码来做测试。

“名小子”的使用方法和“啊D注入工具”法类似，这里就不详细介绍了，如图6-65所示。



【图6-65】名小子

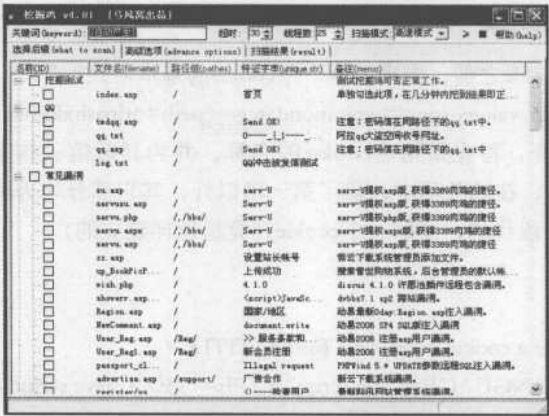
挖掘鸡的使用方法：

一些黑客及黑客软件(包括网站管理员及管理工具)会在网站生成特定路径(目录名+文件名)，这些路径往往有习惯性及默认性。这样的路径在网络中孤立无链接，通过搜索引擎很难直接搜索到。挖掘鸡就是针对这样的路径进行扫描来获取敏感信息或webshell等权限。

比如常见木马上传文件名：明小子旁注在网站/或/bbs/下默认上传diy.asp，内容为简单的上传shell，密码为空；再如常见qq密码信文件名：阿拉QQ大盗在网站/下默认上传tmdqq.asp，用于接收密码信并存储到同路径的qq.txt中。

勾选想要挖的后缀（建议不要太多，1-2个就行），点开始(>)即可(关键词留空的话程序会自动选择热门关键词)，如图6-66所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图6-66】勾选后缀

挖掘鸡使用其实很简单，不过因为有些后缀较少，长时间挖不到结果，导致大家对自己的使用方法产生怀疑。

这里提供验证挖掘鸡正常工作的方法：勾选index.asp后缀（列表中没有的话，可通过“在线更新后缀”功能获取或手工添加），关键词可不填，点开始（>）后数分钟内如果能挖到结果，就说明挖掘鸡正常工作中，唯一缺的就是耐心和更多更有效的后缀了。

漏洞的防范措施

在进行SQL注入攻击前，入侵者需要在可修改参数中提交“'”或“and”等特殊字符，以判断是否存在注入漏洞；在实施SQL注入时，需要提交“；”、“：”及连接号等各种字符构造的SQL注入语句。总之，SQL注入攻击的存在是由于程序员在ASP或其他语言中，将变量在未经过滤和检测的情况下直接引入SQL语句而造成的。

因此防范SQL注入攻击，就要检查对用户的输入，确保用户输入数据的安全性。在具体检查用户输入或提交的变量时，可对单引号、双引号、分号、逗号、冒号和连接号等进行转换或者过滤，这样就可以直接防止此漏洞的产生。

6.3.3 COOKIE欺骗

Cookie记录着用户的帐户ID、密码之类的信息，如果在网上传递，通常使用的是MD5方法加密。这样经过加密处理后的信息，即使被网络上一些别有用心的人截获，也看不懂，因为他看到的只是一些无意义的字母和数字。然而，现在遇到的问题是，截获Cookie的人不需要知道这些字符串的含义，他们只要把别人的Cookie向服务器提交，并且能够通过验证，就可以冒充受害人的身份，登录网站。这种方法叫做Cookie欺骗。Cookie欺骗实现的前提条件是服务器的验证程序存在漏洞，并且冒充者要获得被冒充的人的Cookie信息。目前网站的验证程序要排除所有非法登录是非常困难的，例如，编写验证程序使用的语言可能存在漏洞。

现在有很多社区网为了方便网友浏览，都使用了cookie技术以避免多次输入密码，所以只要对服务器递交给用户的cookie进行改写就可以达到欺骗服务程序的目的。

一、cookie的建立

在讲如何建立cookie之前，先来了解一下cookie的基本格式：

cookieName+cookieValue;expire=expirationDategmt;path=urlpath;domain=sitedomain

其中各项以;分开，首先是指定cookie的名称，并为其赋值。接下来分别是cookie的有效
期，url路径以及域名，在这几项中，除了第一项以外，其它部分均为可选项。

下面我们来看一段代码，了解一下cookie究竟是怎样建立的：

```
<HTML>
<HEAD>
<TITLE>Set a cookie based on a form</TITLE>
<SCRIPT LANGUAGE="java script" TYPE="TEXT/java script">
<!-- Hide script from older browsers

    expireDate = new Date
    expireDate.setMonth(expireDate.getMonth()+6)

    userName = ""
    if (documents.cookie != "") {
        userName = documents.cookie.split("=")[1]
    }

    function setCookie() {
        userName = document.myform.nameField.value
        documents.cookie = "userName="+userName+";expires=" + expireDate.toGMTString()
    }

    // End hiding script -->
</SCRIPT>
</HEAD>
<BODY BGCOLOR="WHITE" onLoad="document.myform.nameField.value =
userName">
    <form NAME="myform">
        <H1>Enter your name:<INPUT TYPE="TEXT" NAME="nameField"
onBlur="setCookie()"></H1>
    </form>
</BODY>
</HTML>
```

这是一段简单的建立cookie的脚本。

(1) `<SCRIPT LANGUAGE="java script" TYPE="TEXT/java script">`

脚本开始的标记，这一句告诉浏览器以下将是java script。

(2) `<!-- Hide script from older browsers>`

为了防止浏览器不能识别脚本，而让浏览器误以为是HTML注释而忽略它。

(3) `expireDate = new Date`

获取当前日期，并存入变量expireDate中。

(4) `expireDate.setMonth(expireDate.getMonth()+6)`

获取当前月份值，将其加6后设置为expireDate的月份总值部分。这意味着本cookie的有效期为6个月。

(5) `if (documents.cookie != "")`

如果document的值不为空，相当于检查用户硬盘上是否已经有了cookie。

(6) `userName = documents.cookie.split("=")[1]`

此处用到了split("=")函数，它的功能是把cookie记录分割为数组，cookie的名为cookie[0]，值为cookie[1]，以此类推。所以此处documents.cookie.split("=")[1]返回的值是此cookie的值。在此句中将值赋给了变量username。

(7) `function setCookie()`

设置名为setCookie的函数。

(8) `documents.cookie = "userName="+userName+";expires="+ expireDate.toGMTString()`

此句是将设置好的cookie写入用户硬盘。expireDate.toGMTString()把expireDate中的值转换为文本字符串，这样才能写入cookie中。

(9) `onLoad="document.myform.nameField.value = userName"`

当页面载入时，把username的值写入文本框(如果有的话)。

(10) `onBlur="setCookie()`

当用户离开文本框时，onBlur调用函数setCookie。

结合上面的注释，读那段代码相信不成问题吧!既然可以建立cookie，那么读取也不是什么难事，请接着往下看!

二、读取和显示cookie

一般来说，cookie的作者并不希望cookie被显示出来，但是要了解cookie，必须要读出其意义。

```
<HTML>
```

```
<HEAD>
```

```
<TITLE>Cookie Check</TITLE>
```

```
</HEAD>
```

```
<BODY BGCOLOR="WHITE">
```

```
<H2>
```

```
<SCRIPT LANGUAGE="java script" TYPE="TEXT/java script">
```

```
<!-- Hide script from older browsers
```

```
if (documents.cookie == "") {  
    document.write("There are no cookies here")  
}  
else {  
    thisCookie = documents.cookie.split(";")  
  
    for (i=0; i<thisCookie.length; i++) {  
        document.write("Cookie name is ' "+thisCookie.split("=")[0])  
        document.write("' , and the value is ' "+thisCookie.split("=")[1]+' <BR>")  
    }  
}  
  
// End hiding script -->  
</SCRIPT>  
</H2>  
</BODY>  
</HTML>
```

以上便是一段读取cookie的名字和值的脚本。上文中解释过的语句在此不多赘述，且看有什么新的语法：

(1) thisCookie = documents.cookie.split(";") [注意：并非前文中出现过的split("=")。

split(";")可以产生数组的结果，本句中，由documents.cookie.split(";")来获取cookie的值，并将这个数组赋值给带变量：thisCookie。

(2) for (i=0; i<thisCookie.length; i++)

设置计数器变量i的值为0，如果它的值小于thisCookie.length(thisCookie中值的个数)，将i的值加1。

(3) document.write("Cookie name is ' "+thisCookie.split("=")[0])

此句中thisCookie.split("=")[0]较难理解，上面的脚本中，thisCookie已经被赋值为一个数组的值，那么thisCookie是指数组中第i个值，也就是第i个cookie，而由上文可知split("=")[0]是指cookie的名字。

这样thisCookie.split("=")[0]便是第i的cookie中cookie的名字！

(4) document.write("' , and the value is ' "+thisCookie.split("=")[1])

跟3极为相似，即是第i个cookie中 cookie的值。

到此，我们已经熟悉了如何建立cookie以及它的读取。这些也正是cookie欺骗也需要的主要技术！

三、cookie欺骗的实现

要做到cookie欺骗，最重要的是理解目标cookie中的储值情况，并设法改变它。由上面的学习我们知道，基于cookie的格式所限，一般来说，只有在Cookie.split("=")[0]和Cookie.

split("=")[1]中的值才是有用的。也就是说只需改变这两处或是处的值即可达到目的。

而在实际操作中，还得先解决另一个问题。由于受浏览器的内部cookie机制所限，每个cookie只能被它的原服务器所访问！我们总不能跑到人家服务器上操作吧！这里就需要一个小技巧了。

在上面我们提到过cookie的格式，最后两项中分别是它的url路径和域名。不难想到，服务器对cookie的识别靠的就是这个！

而在平时要浏览一个网站时，输入的url便是它的域名，需要经过域名管理系统dns将其转化为IP地址后进行连接的。这其中就有一个空当。如果能在dns上做手脚，把目标域名的IP地址对应到其它站点上，我们便可以非法访问目标站点的cookie了！

做到这一点并不难，当然我不并不是要去操纵dns，而且那也是不可能的事情。在win9下的安装目录下，有一名为hosts.sam的文件，以文本方式打开后会看到这样的格式：

```
127.0.0.1 localhost #注释
```

利用它，我们便可以实现域名解析的本地化！而且优先权高于网络中的dns！

具体使用时，只需将IP和域名依上面的格式添加，并另存为hosts即可！（注意：此文件无后缀名，并非hosts.sam文件本身！）

到此，cookie欺骗所需的所有知识已经齐备。下面以一个“假”的例子，演示一下如何进入实战。

假设目标站点是 www.xxx.com

www.self.com是自己的站点。（可以用来存放欺骗目标所需的文件，用来读取和修改对方的cookie。）

首先ping出www.self.com的IP地址：

```
ping www.self.com
```

```
Reply from 12.34.56.78: bytes=32 time=20ms TTL=244
```

然后修改hosts.sam文件如下：

```
12.34.56.78 www.xxx.com
```

并保存为hosts。

将用来读取cookie的页面传至www.self.com（脚本如二所示）。

此时连上www.xxx.com。由于已经对hosts动过手脚，这时来到的并不是www.xxx.com，而是www.self.com

www.xxx.com没在本地的cookie便可被读出。

然后根据具体情况修改一的脚本，用同样的方法，向此cookie中写入数据。修改完毕后，删掉hosts文件，再重新进入www.xxx.com，此时已经大功告成，可享受你的hack成果了。

6.3.4动网上传利用程序

动网论坛是目前网上最流行的论坛系统之一。漏洞层出不穷，这里我们还是利用最原始的上传漏洞来入侵。

【案例6-8】利用上传漏洞入侵动网

(1) 打开一个采用动网论坛程序的论坛，首先注册一个用户名，如图6-67所示。



【图6-67】注册用户名

(2) 注册完了用户名以后，在论坛上登录，选择“用户控制面板”→“基本资料修改”，如图6-68所示。



【图6-68】选择基本资料修改

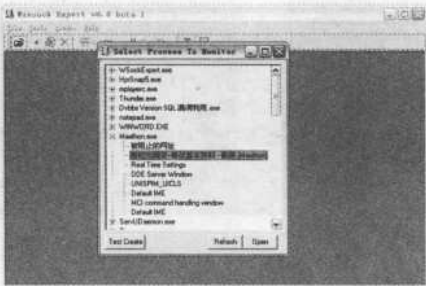
(3) 打开“用户基本资料修改”页面，在头像框，单击“浏览”按钮，选择一个asp文件，此时先不要单击“上传”按钮，如图6-69所示。



【图6-69】修改基本资料

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(4) 运行抓包工具：WSockExpert.exe抓修改基本资料的数据，选择浏览器打开的修改基本资料页面，单击“Open”按钮，如图6-70所示。



【图6-70】运行抓包工具

(5) 这时切换到浏览器窗口，点击“上传”按钮，抓包工具就会抓到很多数据包，其中一个数据包，就截取到了上传页面，以及Cookie，如图6-71所示。



【图6-71】抓取到上传页面和Cookie

(6) 然后用桂林老兵的DVBBS上传利用程序，填写相应的内容，提交地址和Cookie就是刚才抓取到的，如图6-72所示。本地文件，就是本地asp木马，asp木马的制作，这里就不再赘述。



【图6-72】DVBBS上传利用程序

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

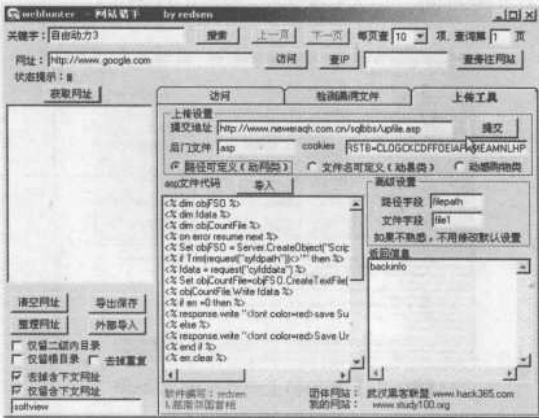


(7) 上传成功后，运行刚才上传的asp木马，发现打开页面，如图6-73所示。说明管理员做了修补，上传并不成功。



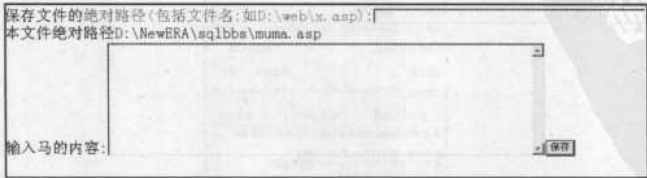
【图6-73】页面上传不成功

(8) 换一种上传工具，选择“网站猎手”，提交地址、后门文件、Cookie像刚才一样设置，并且选择“路径可定义（动网类）”，如图6-74所示，设置完成后，单击“提交”按钮。



【图6-74】网站猎手

(9) 程序提示上传成功以后，再次在浏览器中打开上传的asp页面，这次成功了，如图6-75所示。



【图6-75】打开上传的asp文件

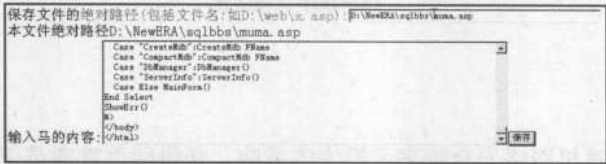
(10) 用记事本打开在桂林老兵站下载的asp木马，如图6-76所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



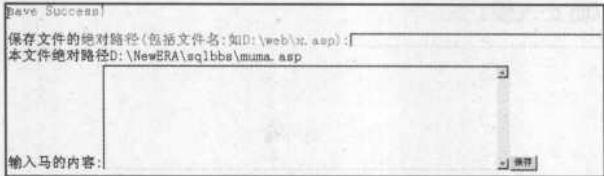
【图6-76】用记事本打开asp文件

(11) 选择所有的代码，复制到已经上传的asp页面中“输入马的内容”对话框中，保存文件路径可以参考“本文件的绝对路径”，在页面部分，换一个名字即可，如图6-77所示。



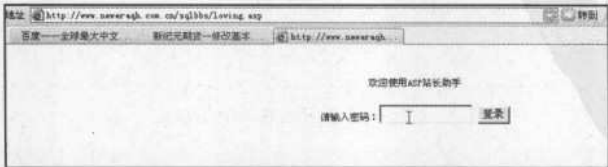
【图6-77】上传木马

(12) 单击“保存”按钮，出现“Save Success!”提示，说明，上传成功，如图6-78所示。



【图6-78】上传成功

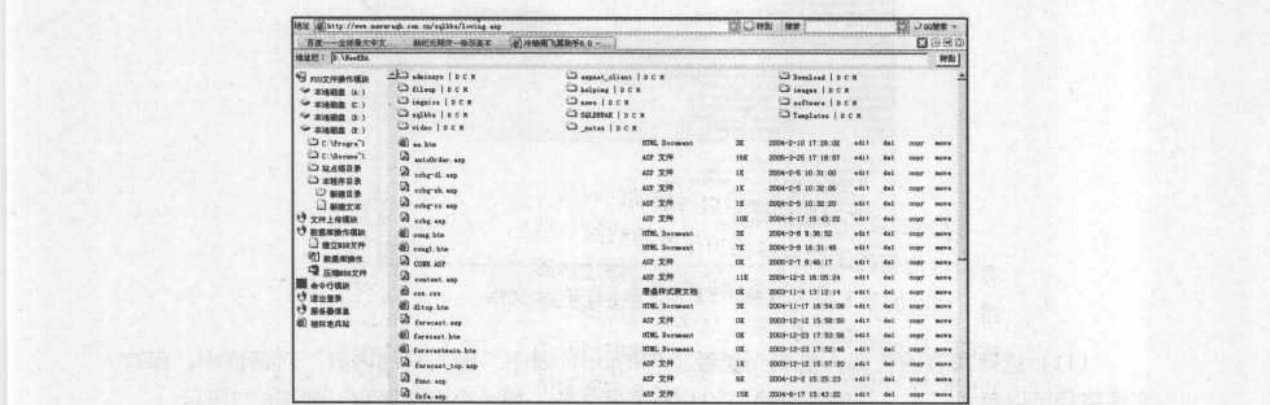
(13) 打开刚才上传的木马页面，输入密码登录。密码在记事本打开源代码中，可以查询到，如图6-79所示。



【图6-79】运行木马

黑客
兵刃大曝光

(14) 输入正确的密码以后, 就可以看见网站的所有页面, 并可以更改页面内容了, 如图 6-80 所示。



【图6-80】入侵成功

6.4 小结

网页破解给计算机网络安全带来了极大的威胁，获得网页管理员密码和后台控制权之后，就可以随意修改网页内容，查看用户资料。今年轰动一时的海南大学骗录案就是黑客入侵海南大学主页之后修改了内容来冒充海南大学录取学生的。

网页入侵的切入点都是网页自身的漏洞,所以在网页的设计和维护过程中要规范操作,尽量将漏洞堵住,以防止入侵。

第7章 文档密码破译工具

在对安全和保密的需求日益增加的时代，有很多加密的工具能够保护作者的利益，但是，这些加密工具也受到来自密码破译工具的挑战。在忘记密码的时候，破译工具也是一个找回密码的途径，所以，破译工具的发展并不亚于加密工具，在本章中将介绍各个方面常用的密码破译工具。

本章要点

- 密码破译的方法和工具
- 密码破译工具的防范
- EFS技术

7.1 密码破译工具

密码破解需要工具的支持，很难想象用户一个一个的尝试密码，像是大海捞针。有经验的黑客，会有自己的密码字典，或者使用现成的工具或者自己编写一条小的程序来破解密码。破解密码有很多的技巧，目前也有很多的小软件，能够让你在几秒钟以内免除麻烦的编程过程，但这只适用于简单的密码破解。

7.1.1 显示星号密码工具

密码输入界面中显示输入的密码一般都是暗码，即星号，如果能够显示这些星号背后的密码就能破译了，当然，条件是在已经输入密码并且显示的是星号的密码输入框。下面以案例的形式介绍两个查看星号密码的工具。

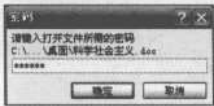
【案例7-1】用XP密码查看器查看星号密码。

XP密码查看器可以用来查看显示Windows XP系统下的密码，例如Word文档和Excel报表的密码，具体使用如下：

- (1) 安装XP密码查看器，然后打开，弹出XP密码查看器主界面，如图7-1所示。
- (2) 本例中要显示的是一个名为“科学社会主义”文档的打开密码，如图7-2所示，输入的密码是以星号的形式来显示的。

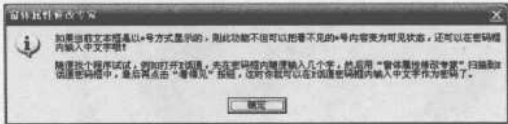


【图7-1】XP密码查看器主界面

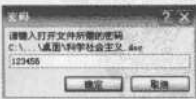


【图7-2】带密码的文档

- (3) 单击图7-1中XP密码查看器主界面的“看得见”按钮，弹出说明窗口，如图7-3所示。单击“确定”按钮。
- (4) 此时，再观察刚才的文档密码输入窗口，星号已经变为了明码显示，如图7-4所示。



【图7-3】说明窗口



【图7-4】显示明码

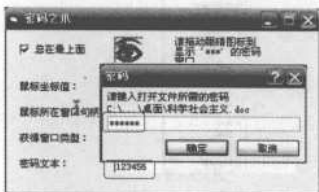
【案例7-2】利用密码之爪显示星星背后的密码原文

密码之爪也是一个显示星号后面密码原文的工具软件，使用也比较简单。具体使用如下：

- (1) 安装密码之爪，安装好之后打开程序，弹出密码之爪的主界面，如图7-5所示。
- (2) 用鼠标左键按住眼睛图标拖动到星号密码的位置，就可以看到星星背后的密码原文，并且还能显示出当时鼠标所在位置的窗口句柄，窗口类型，将鼠标拖动到上例中“科学社会主义”文档的星号密码上，看到密码的原文明码，如图7-6所示。



【图7-5】密码之爪主界面



【图7-6】显示密码原文

7.1.2 Windows操作系统登录密码破译

Windows操作系统可以设置登录密码，然而用很多方法可以绕过登录密码登录，这为非法进入者的登录提供了机会，也为忘记密码时候登录提供了可行的方法。下面来看哪些方法能够破译Windows操作系统的登录密码。

1. 删除SAM文件清除管理员密码

- (1) 直接清除用户口令文件

相关情况：无任何用户账号（包括管理员Administrator的账号）、无输入法漏洞等可利用漏洞。

第一步，使用Windows2000或者XP启动光盘的修复功能，或者其他可以引导进入DOS状态的光盘引导系统，并进入DOS状态。

第二步，进入目录 %root%\system32\config\（%root% 指Windows主目录，一般是C盘的Windows目录），手动删除该目录下的SAM文件。

第三步，重新启动计算机，再次进入Windows的时候，不需要密码便能以管理员身份直接进入系统了。

- (2) 利用系统输入法漏洞

相关情况：无任何用户账号（包括管理员Administrator的账号），但在登录时打开输入法，利用输入法工具条可进入到输入法的帮助界面。

【案例7-3】以紫光输入法为例，说明如何利用输入法漏洞。

- (1) 在输入法工具条上单击右键，单击“帮助”，如图7-7所示。
- (2) 在打开的“联机帮助”对话框中，单击左上角的图标，选择“跳至URL”，如图7-8所示。

2. 用ERD Commander 2003恢复Windows XP密码

ERD Commander 2003是一款可以轻松修改系统管理员密码的傻瓜化软件，而且这款软件对Windows 2000/XP/2003各种版本的系统均有效。

【案例7-4】使用ERD Commander 2003恢复Windows XP密码。

利用ERD2003强行修改系统管理员密码，对2000/XP/2003系统均有效。下面就具体介绍一下它的用法。

- (1) 首先要下载ERD2003，把它刻录成CD，记录过程这里就不详细介绍了。
- (2) 光盘启动进入画面，它很像Windows XP的启动画面，如图7-11所示。



【图7-11】ERD2003启动画面

- (3) 进入“系统”后，ERD2003会针对系统的网络等硬件设备进行一些设置，可以一律先“Yes”。

- (4) 接下来，ERD2003会在你的硬盘里搜索所有已安装的系统，再让你选择要修改的系统，如图7-12所示。



【图7-12】系统登录框

- (5) 选择要登录的系统后，单击“确定”按钮，就正式进入ERD2003桌面，和XP的桌面非常相似，如图7-13所示。



【图7-13】ERD2003系统界面



(6) 选择“开始”→“管理工具”→“修改密码”命令，进入强行修改密码的界面，随后弹出“修改密码”对话框，选择要修改密码的用户名，再选择修改密码而不用输入原始密码，然后单击“下一步”按钮，如图7-14所示。



【图7-14】修改密码

(7) 出现“完成”对话框，单击“Finish”按钮，重新启动计算机。试试用你修改的密码登录。到此，即成功用ERD2003破解了用户的登录密码。这种方法对于忘记了登录密码非常适用，只要有了ERD Commander 2003，就有了一把登录Windows系统的万能钥匙。

3. 妙用密码重设盘

如果忘记了Windows XP的登录密码，该怎么办呢？为了避免尴尬发生，通过“忘记密码向导”创建“密码重设盘”是个有效的方法。下面介绍“密码重设盘”的创建和使用。

【案例7-5】创建“密码重设盘”。

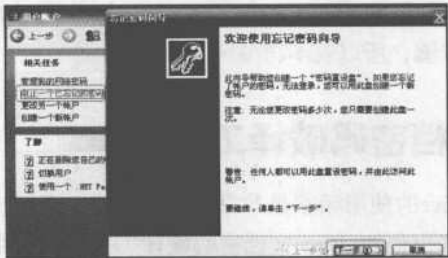
(1) 单击“开始”→“设置”→“控制面板”，打开控制面板窗口，双击“用户账户”。在弹出的“用户账户”对话框中单击账户名称，例如“Administrator”，如图7-15所示。



【图7-15】选择一个账户

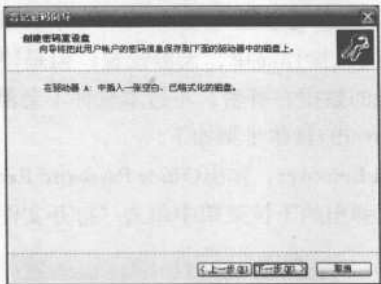
(2) 在弹出的“用户账户”窗口的“相关任务”栏下方，单击“阻止一个已忘记的密码”，弹出“忘记密码向导”窗口。单击“下一步”按钮，如图7-16所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



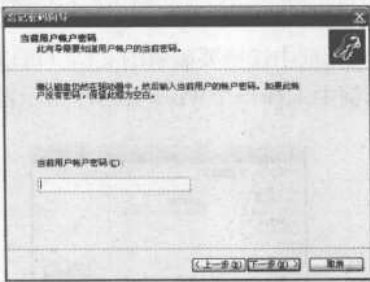
【图7-16】忘记密码向导

(3) 在软驱中插入一张空白的、已格式化的软盘，单击“下一步”按钮，如图7-17所示。



【图7-17】插入空白软盘

(4) 输入当前用户的账户密码，然后单击“下一步”按钮，如图7-18所示。系统就开始创建密码重置磁盘，最后单击“完成”即可。



【图7-18】输入当前用户的账户密码，开始创建密码重置磁盘

【案例7-6】使用“密码重置盘”。

如果使用的是Windows XP的新式登录界面，在出现欢迎屏幕时，单击用户名，然后输入密码，如果输入了错误的密码，会显示“没有记住密码？”的提示；这时单击其中的“使用密码重置磁盘”，就会打开“密码重置向导”；单击“下一步”按钮，插入已经创建的“密码重置盘”；再单击“下一步”按钮，输入新密码及确认密码；单击“下一步”，最后单击“完成”按钮即可。这样新密码就代替了旧密码。

如果使用的是传统的登录界面，在登录界面“密码”栏中输入错误密码后，会弹出“登

录失败”对话框，单击“重设”按钮即可利用“密码重设盘”设置新的密码，具体步骤同上例中创建“密码重设盘”的步骤，所以就不再赘述。

7.1.3 Office文档密码破译工具

日常办公和生活中Office的使用频率是非常高的，设置密码后忘记的情况也非常多，其实忘记密码并不可怕，有众多出色的Office文档密码破译工具可以适用，而且都比较易于操作，耗时也不多，对于紧要的被忘记密码的Office文档可以适用下面介绍的几种工具来打开。

【案例7-7】使用Office Password Remover恢复Word密码。

Office Password Remover是一款可以瞬间破解 Word、Excel和Access 文档密码的工具，一般情况下解密过程不超过5秒，而且操作简单，无需设置。但是使用本软件需要连接到互联网，因为要向软件服务器发送少量的数据并解密，不过本软件不会泄露任何个人隐私，可以放心使用。使用Office Password Remover的具体步骤如下：

(1) 打开Office Password Remover，弹出Office Password Remover主界面，界面很简洁，单击菜单栏的“文件”菜单，在弹出的下拉菜单中单击“打开文件”如图7-19所示。



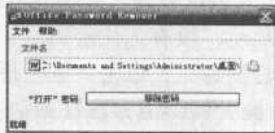
【图7-19】Office Password Remover主界面

(2) 在弹出的“打开”对话框中选择要破解的文档（可以是Office系列的任何一个文档，包括Word、Excel文档等）本例中选择一个Word文档作为示范，选择好之后单击“打开”按钮，如图7-20所示。



【图7-20】选择要破解的Office文档

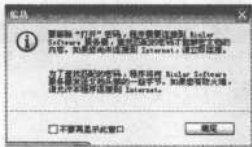
(3) 在弹出的“Office Password Remover”窗口中单击“移除密码”按钮，如图7-21所示。



【图7-21】移除密码

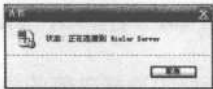
第 7 章 文档密码破译工具

(4) 弹出信息，询问是否发送一些字节到服务器以取得密码，单击“确定”按钮，如图 7-22所示。



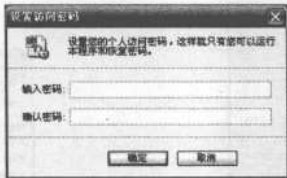
【图 7-22】发送信息

(5) 弹出“连接”窗口，显示状态是正在连接到破解服务器，连接成功后会返回一个状态信息，返回破解出来的密码，如图 7-23所示。



【图 7-23】连接到服务器进行破解

(6) 如果担心其他用户进入计算机后利用Office Password Remover来破解本机上的文档，可以对Office Password Remover设置保护密码，在主界面中单击“文件”菜单，在弹出得下拉菜单中单击“设置访问密码”就会弹出“设置访问密码”对话框，如图 7-24所示，在此对话框中输入密码然后单击“确定”按钮就可以了，这样就需要密码才能打开和使用Office Password Remover了。



【图 7-24】设置Office Password Remover的访问密码

【案例 7-8】用WORD97/2000/XP密码查看器找回密码。

WORD97/2000/XP密码查看器是一个专用于Word文档的密码找回工具，使用的具体步骤如下：

(1) 打开WORD97/2000/XP密码查看器，弹出WORD97/2000/XP密码查看器主界面，单击菜单栏的“文件”菜单，在弹出的下拉菜单中单击“打开”按钮，如图 7-25所示。

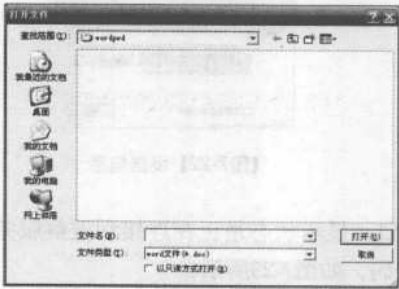


【图 7-25】WORD97/2000/XP密码查看器主界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



(2) 在弹出的“打开文件”对话框中选择要破解的文档，然后单击“打开”按钮，如图7-26所示。



【图7-26】“打开文件”对话框

(3) 在弹出的“任务属性”对话框中选择破解的类型，本例中选择“暴力破解”，还可以设置密码的类型，例如“数字”，密码有多少位等，设置得越精确破解的精确度也就越高。设置好之后单击“确定”按钮，如图7-27所示。

(4) 在主界面中单击“操作”菜单，在弹出的下拉菜单中单击“开始破解”进行破解，如图7-28所示。

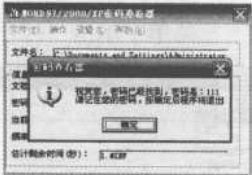


【图7-27】“任务属性”对话框



【图7-28】开始破解

(5) 破解过程中主界面会显示估计剩余时间等信息，破解成功后会弹出“密码查看器”窗口，显示密码，如图7-29所示。



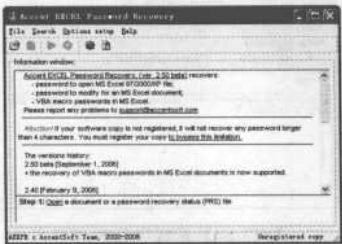
【图7-29】破解成功

【案例7-9】使用Excel Password Recovery轻松找回Excel文档密码。

第 7 章 文档密码破译工具

忘记Excel文档密码的时候可以使用Excel Password Recovery来破解Excel文档，找回密码。
使用Excel Password Recovery来破解Excel文档具体步骤如下：

(1) 打开Excel Password Recovery，弹出它的主界面，在主界面中有菜单栏、工具栏和“Information window（消息窗口）”，如图7-30所示。



【图7-30】Excel Password Recovery主界面

(2) 单击工具栏的文件夹图标，在弹出的“打开”对话框中选择需要解密的Excel文件，然后单击“打开”按钮，如图7-31所示。



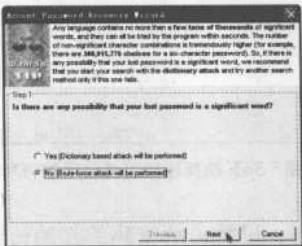
【图7-31】打开需要解密的文档

(3) 此时，主界面中工具栏的三角形按钮变成绿色，单击此绿色按钮，开始进行解密设置，如图7-32所示。



【图7-32】工具栏中的绿色三角形按钮

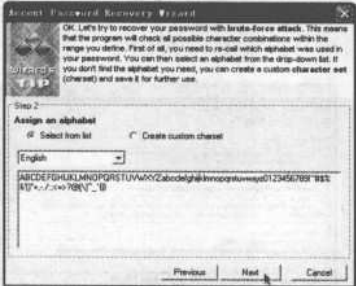
(4) 进入破解设置的第一步，Excel Password Recovery询问丢失的密码是否有意义，如果有意义就单击“Yes（是）”，进行字典破解；如果设置的密码没有一定意义就单击“No（否）”进行暴力破解。本例中选择暴力破解，单击“Next（下一步）”按钮，如图7-33所示。



【图7-33】选择破解方式

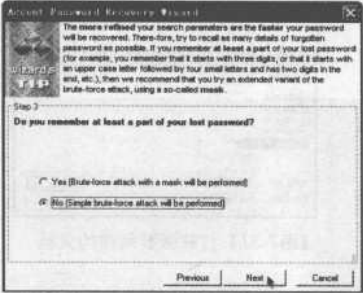
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(5) 进入破解设置的第二步，选择字母表和语言，此步骤可以保持默认选项，设置好之后单击“Next（下一步）”按钮，如图7-34所示。



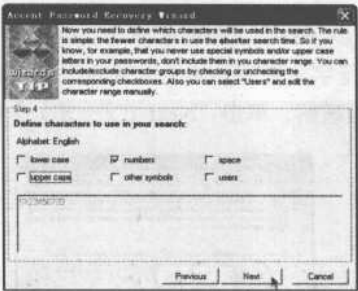
【图7-34】选择字母表和语言

(6) 进入破解设置的第三步，Excel Password Recovery询问是否记得密码中的一部分，如果不记得也没有关系，单击“No（否）”，采用简单暴力破解，如图7-35所示。



【图7-35】进一步选择破解方式

(7) 进入破解设置的第四步，选择密码可能使用的符号类型，勾选可能的符号类型。例如，如果知道密码是全数字的，则只勾选“numbers（数字）”，然后单击“next（下一步）”按钮，如图7-36所示。



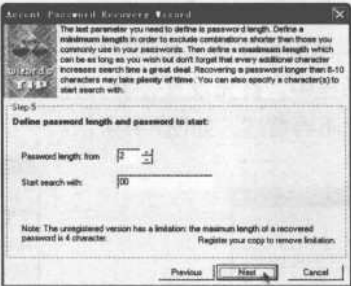
【图7-36】选择密码可能使用的符号类型

(8) 进入破解设置的第五步，设置破解密码的起始长度和开始的密码，例如设置从两个

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

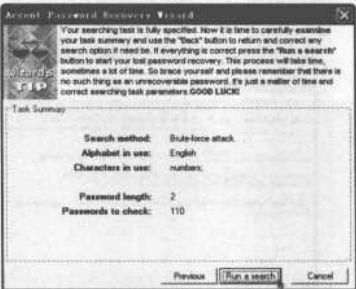
第 7 章 文档密码破译工具

字符长度的密码“00”开始破解，如图7-37所示。



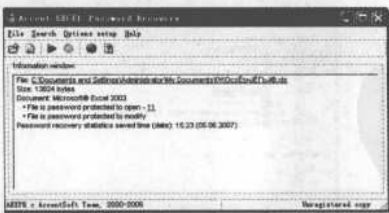
【图7-37】设置破解密码的起始长度和开始的密码

(9) 弹出任务概要窗口，在此可以看到设置的内容，如果不满意现在的设置，可以单击“Previous（回顾）”按钮，返回上面步骤重新设置，满意以后单击“Run a search（开始搜索）”按钮，如图7-38所示。



【图7-38】任务概要窗口

(10) 破解完成后在“Information window（消息窗口）”会显示密码信息，本例中显示文档的打开权限密码为“11”，如图7-39所示。



【图7-39】破解成功

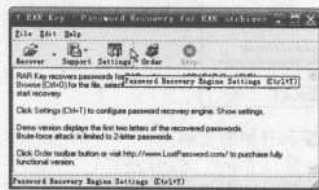
7.1.4 用RAR Key 轻松打开加密RAR压缩文件

【案例8-10】运用 keyRAR解密。

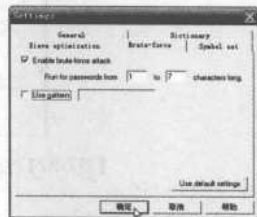


运用RAR文件解密工具（RAR key）来进行RAR文件的解密。使用RAR key解密RAR文件的具体步骤如下：

（1）打开RAR key，在弹出的主界面工具栏中单击“Settings（设置）”工具，如图7-40所示。在弹出的“Settings”对话框中，首先设置破解的类型等参数，在前面的几种破解工具中都已经介绍过参数设置了，在此不再赘述，如图7-41所示。

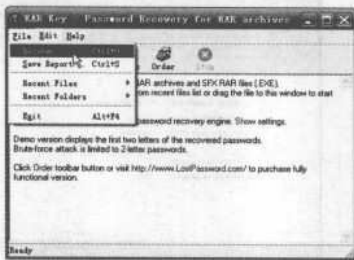


【图7-40】RAR key主界面



【图7-41】Settings对话框

（2）主界面中单击菜单栏的“File（文件）”按钮，在弹出的下拉菜单中单击“Recover（重新找到）”如图7-42所示。



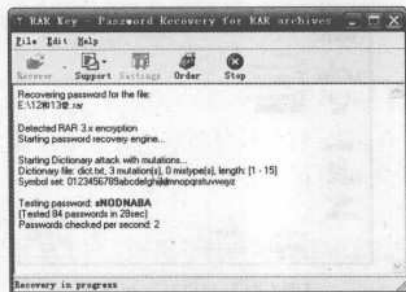
【图7-42】打开文件

（3）弹出“Select file to recover（选择要找到密码的文件）”，选择好需要破解的RAR文件之后单击“打开”按钮，如图7-43所示。



【图7-43】打开要解密的RAR文件

（4）上一步中选择的文件出现在主工作区中，破解开始，如图7-44所示。和前面讲解过的Advanced RAR Password Recovery一样，破解完毕之后弹出一个对话框，显示密码已经成功破解，在“Password for the file（文件的密码）”栏中显示的就是密码。



【图7-44】破解

7.1.5 Advanced PDF Password Recovery

PDF (Portable Document Format) 文件格式是电子发行文档的常用格式，越来越多的电子图书、产品说明、公司文告、网络资料、电子邮件都在使用PDF格式文件。如果急需一个PDF文件，但是又忘了密码，可以使用PDF Password Recovery来解决这个问题。

PDF Password Recovery 可以用来解密已设密码的 Adobe Acrobat PDF 文件，像设定了“拥有者”的密码，已解密的档案可以不受限制地被任何 PDF 阅读器打开（例如：Adobe Acrobat Reader）。然后可以轻松地进行编辑、复制、打印操作。

【案例8-11】使用PDF Password Recovery解密PDF文档。

使用PDF Password Recovery解密PDF文档的具体步骤如下：

- (1) 打开PDF Password Recovery，弹出PDF Password Recovery主界面，单击此界面的左上方菜单栏中的“打开”按钮，如图7-45所示。



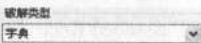
【图7-45】PDF Password Recovery主界面

- (2) 在弹出的“打开”对话框中选择将要加密的PDF文档，然后单击“打开”按钮，如图7-46所示。



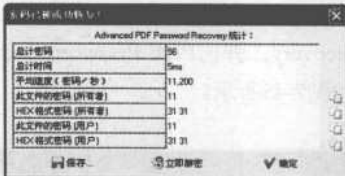
【图7-46】“打开”对话框

(3) 在主界面中“破解类型”栏的下拉菜单中选择破解类型，本例中选择“字典”破解，如图7-47所示。因为一般的破解软件都会有一个字典，包含可能的密码，选择“字典”破解时，破解软件会从该字典中取出密码进行尝试。选择好破解类型后在主界面的菜单栏单击“开始”按钮。



【图7-47】选择破解类型

(4) PDF Password Recovery开始进行破解，完毕后弹出“密码已被成功恢复”对话框，可以从中读出加密的PDF文档的用户密码和所有者密码均为“11”，该对话框中还有“总计密码”、“总计时间”等破解信息，如图7-48所示。单击“确定”完成破解。



【图7-48】成功破解密码

7.1.6 BIOS密码破解

为了防止其它人未经允许使用我们的计算机，大部分主板都允许设置BIOS密码。BIOS被设置密码之后一般会有两种情况：

1. 开机能够引导进入系统

第一种开机后可以引导系统，但当企图修改BIOS设置时会被提示输入密码，如密码错误将无法更改BIOS设置。

任何一个系统，一般都留有后门，CMOS也不例外。

所谓万能密码，就是BIOS程式上面的Back Door，通常厂商用来方便自己的工程人员使用，所以万能密码可以无论你设什么密码，都能进入BIOS重新设定。每个厂家各个时期的万能密码都不同，此法并不能常常奏效。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(1) 通用密码法

AMI 的BIOS常有：AMI ; Sysg, PASSWORD, HEWITT RAND, AMISW, AMI_SW, LKWPETER, aammii, AMIISW, AMIPSWD, AMLKEY, amipswd, ami.kez,

AMISSETUP, AMI~, bios310, ami, BIOSPASS, amiami, CMOSPWD, amidecod, HEWITT, RAND, KILLCMOS.

AWARD的BIOS常有：award , Syxz, h996, wantgirl, eBBB, dirrid, 1EAAh, 256256, 589589, 589721, admin, alfarome, aLLy, aPA, awkward

phoenix BIOS常有：phoenix

其它品牌机上的万能密码			
厂家	密码	厂家	密码
Biostar	Biostar	Q54arwms;	Compaq:
Concord	last	CTX	International
CyberMax	Congress	Daewoo	Daewuu
Daytek	Daytec	Dell	Dell
Digital	Equipment	kompric	Enox
Epox	central	Freotech:	Posterie
HP	Vectra	hewlpack	IBM
Iwill	iwill	JetWay:	spoom1
Joss	Technology	57gbz6	technolgi
MachSpeed:	sp99dd	Magic-Pro:	prost
Megastar	star	Micron	sidkj754
Micronics	dn_04rjc	Nimble:	xdfk9874t3
QDI	QDI	Quantex	teX1
Siemens	Nixdorf	SKY_FOX	SpeedEasy:
TMC	BIGO	Toshiba	24Banc81
Vextrec	Technology	Vextrex	Vobis:

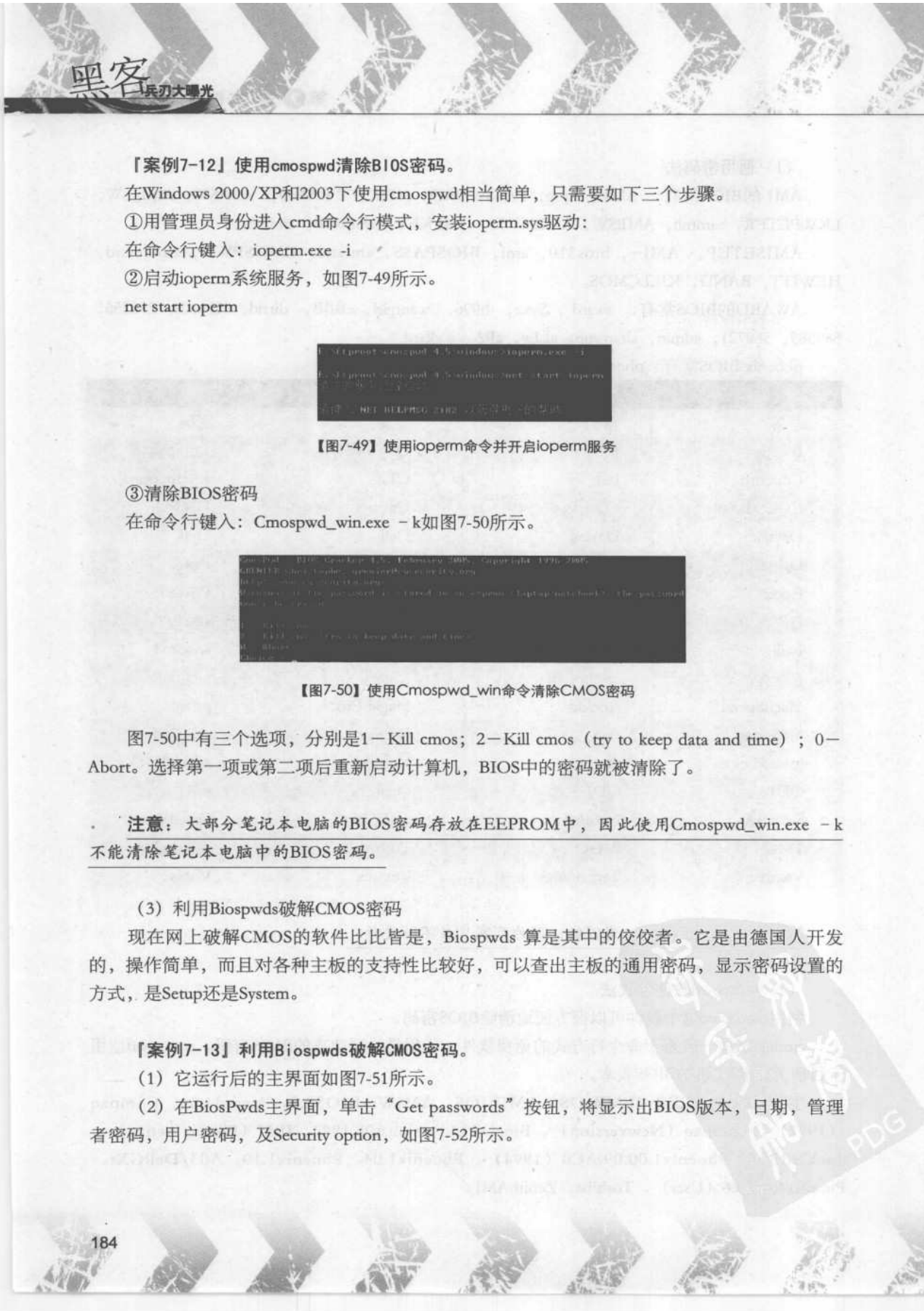
注意：万能密码并不一定万能，因为厂家总在不断更新。

(2) cmospwd软件修改法

利用cmospwd这个软件可以很方便地清除BIOS密码。

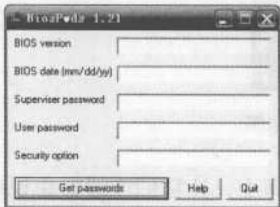
cmospwd是一款基于命令行方式的免费软件，作用是找回遗忘的BIOS密码。cmospwd适用于目前大部分PC机的BIOS版本。

主要包括：ACER/IBMBIOS、AMIBIOS、AMIWinBIOS2.5、Award4.5x、Compaq (1992)、Compaq (Newversion)、BiosDELLversionA08,1993、IBM (PS/2, Activa)、PackardBell、Phoenix1.00.09.AC0 (1994)、Phoenix1.04、Phoenix1.10、A03/DellGXi、Phoenix4release6 (User)、Toshiba、ZenithAMI。

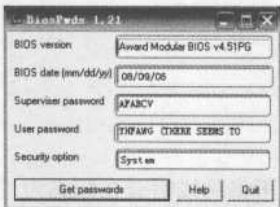


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 7 章 文档密码破译工具



【图7-51】 BiosPwds 主界面



【图7-52】 BiosPwds 应用



BIOSPwds获得的密码并不一定完全正确，而且它得出来的密码可能和原来设置的不同。一般根据主板的版本而定。除了这个BIOSPwds外，还有CMOS小精灵CMOS Cracker，它们的破解密码功能也是非常不错的。应用此种方法的前提是能够进入电脑系统。

2. 开机后提示输入密码

开机后就被提示输入密码，如果密码输入错误根本无法进入系统。此时很难使用软件破解，在通用密码又找不到的情况下，可以考虑从物理硬件上下手。有三种方法。

取出电池

因为BIOS的供电都是由CMOS电池供应的，将电池取出便可切断BIOS电力供应，这样BIOS中自行设置的参数就自动清除。

◆操作步骤如下：

- (1) 关掉电源，打开机箱。
- (2) 在主板上找到CMOS电池插座，然后将插座上那个卡住供电电池的卡扣压向一边，CMOS电池就会自动弹出，将电池小心取出，如图7-53所示。



【图7-53】 拔CMOS电池

(3) 待放电完毕后，再装上CMOS电池，启动电脑，屏幕上就会提示“CMOS checksum error-Defaults loaded”，需要重新进入CMOS设置。

利用放电跳线。现在的大多数主板，都有放电跳线，方便用户放电操作。跳线一般为三针，位于主板CMOS电池插座附近，附有电池放电说明书。严格按照说明书来操作即可。

操作步骤如下：

- (1) 用专用工具将跳线帽从“1”和“2”的针脚上拔出，如图7-54所示。



【图7-54】拔出跳线帽

(2) 再将跳线帽套在标志为“2”和“3”的针脚上，让它们连通，由说明书上可以知道此时状态为“Clear CMOS”，即清除CMOS。经过几秒接触后，即把BIOS恢复到主板出厂时的默认设置。

(3) 再一次把跳线帽由“2”和“3”的针脚上取出，然后套到原来的“1”和“2”针脚上。

(4) 打开电源，开启计算机，即可进入CMOS设置程式。

短接电池插座的正负极

CMOS电池插座有正负两极之分，把它们短接即达到放电的目的。

操作步骤如下：

(1) 首先将主板上的CMOS供电电池取出。

(2) 再使用有导电性能的工具，如螺丝刀等，短接电池插座上的正极和负极就能造成短路，从而达到放电的目的。

注意：某些电脑清除BIOS密码后不能正确引导，如果提示找不到磁盘，则可能是因为在清除BIOS密码时BIOS中关于硬盘的设置也一并被清除了。这时只要进入BIOS，自动检测一下硬盘然后再重新启动即可。

7.1.7 破解加密光盘

很多重要的资料都会使用光盘保存起来，例如财务报表等。这样可以避免例如电脑中毒之类的状况导致资料的丢失。既然是重要的资料，那么保护措施就要搞好，用光盘保存通常会对光盘进行加密。另外，市面上出售的光盘很多也是加密的，例如许多软件的安装盘。在忘记自己加密的光盘的密码的时候和没有光盘密码的时候，如何打开光盘呢？按照黑客提倡共享的思想，就要利用破解光盘工具进行破解。

加密光盘的破解工具有很多种：

1. File Monitor的使用：

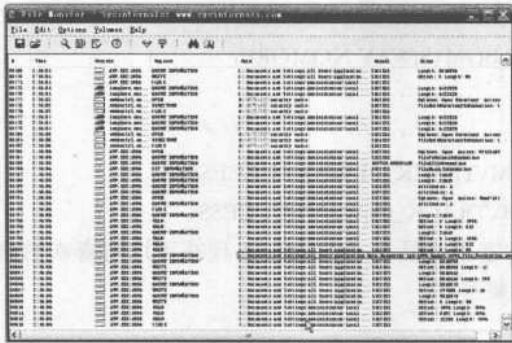
Filemon 是一款出色的文件系统监视软件，它可以监视应用程序进行的文件读写操作。它将所有与文件一切相关操作(如读取、修改、出错信息等)全部记录下来以供用户参考，并允许用户对记录的信息进行保存、过滤、查找等处理，这就为用户对系统的维护提供了极大的便利。利用File Monitor可以知道隐藏目录的加密光盘的目录名称。

当运行Filemon后，它就开始监视系统文件的变化，它可以将输出窗口中的信息保存为一个文件以便于离线浏览。它具有很强的搜索能力，同时如果你发现某些信息是重复的，可以简单地设置一些过滤。利用Filemon的这些功能就可以用来查找加密光盘的目录名称。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

【案例7-14】使用Filemon查找目录的加密光盘。

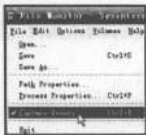
(1) 打开“Filemon”，初次使用它自己就开始运行监视，反映出所有正在运行的程序，如图7-55所示。



【图7-55】File Monitor主界面

(2) 单击菜单栏的“File”，在弹出的下拉菜单中取消勾选“Capture Events”，如图7-56所示。

(3) 为了方便接下来寻找加密的光盘目录，现在将已经记录的系统文件清除掉，单击菜单栏的“Edit”，在弹出的下拉菜单中单击“Clear Display”如图7-57所示。

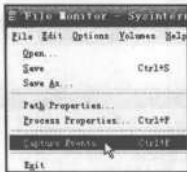


【图7-56】取消勾选“Capture Events”



【图7-57】清除记录

(4) 单击菜单栏的“File”，在弹出的下拉菜单中勾选“Capture Events”，重新开始记录，如图7-58所示。



【图7-58】勾选“Capture Events”

(5) 以某新版DDR跳舞碟为例，运行此光盘。

(6) 回到Filemon，所有的文件调用均被记录下来了。现在将“Capture Events”前面的钩去掉，免得它仍旧不断地增加记录，然后来看看记录的都是什么。以下是截取的部分内容：

Explorer FindOpen E:\DDR99.EXE SUCCESS



```
Explorer FindClose E:\DDR99.EXE SUCCESS
.....

Ddr99 FindOpen E:\BGM\S.WAV NOMORE
Ddr99 FindOpen E:\BGM\S.WAV NOMORE
.....

Ddr99 Open E:\BGM\TRACK_01.WAV SUCCESS
Ddr99 Seek E:\BGM\TRACK_01.WAV SUCCESS

原来此跳舞碟的加密子目录为“BGM”。现在可以将喜欢的曲目拷贝下来了。这样，
Filemon让隐藏目录无处藏身了。
```

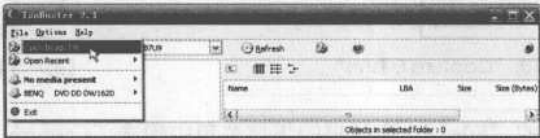
2. IsoBuster的使用：

IsoBuster是一个能够将 TAO、DAO、ISO、BIN、IMG、CIF、FCD 等镜像文件内容直接抓取出来的免费工具。支持各种软件所制作的镜像文件，有 Nero、Duplicator、BlindRead、Easy-CD Creator、CDR-Win、Virtual CD-ROM、CloneCD 等，还可以将 Video CD 的 DAT 文件转换成 MPG 文件。

【案例7-15】使用 IsoBuster浏览光盘上的隐藏文件

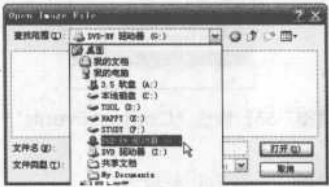
使用IsoBuster浏览光盘上的隐藏文件的具体步骤如下：

(1) 打开IsoBuster，在主界面的菜单栏中单击“File”在弹出的下拉菜单中单击“Open Image File”，如图7-59所示。



【图7-59】 IsoBuster主界面

(2) 在弹出的“Open Image File”对话框中选择要浏览的文件，然后单击“打开”按钮，如图7-60所示。



【图7-60】 选择要打开的文件

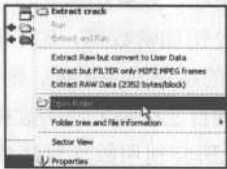
(3) 文件出现在工作区中，在此案例中打开的是在案例29中用光盘加密大师加密的文件，其中有一个隐藏文件、一个超大文件和一个目录变成的文件，这三个文件现在还不能查

看，在文件夹前面被打上了红色的十字符号，如图7-61所示。



【图7-61】显示打开的文件

(4)在打叉的文件上单击右键，在弹出的下拉菜单中单击“Open folder”，如图7-62所示。



【图7-62】打开文件

(5)隐藏的文件出现在工作区了，这样就可以对这些文件打开、执行或者复制了，如图7-63所示。

Name	LBA	Size	Size (Bytes)	Modified
allc.upd	259	22.36 KB	22,901	2003-11-15 18:47:34
crack.txt	271	0.22 KB	221	2004-10-16 20:00:50
rational_pgm.dat	272	25.93 KB	26,583	2004-10-10 17:32:02

【图7-63】显示隐藏的文件

7.2 密码破译工具防范

俗话说“魔高一尺，道高一丈”，虽然密码破解工具的功能都是非常强大，然而还是可以通过一定的防范措施来避免被破解。

7.2.1 防范原理和手段

密码的破解花样可谓繁多，在这样一个环境下面，我们的安全和隐私得不到保障，作为应对之策，只能在加密上面下功夫，使密码更加复杂，更难于被破解。加密机制的改进和密码保护的完善都是对付密码破解的好办法。

针对各种破译软件的特性，这里提出三种比较有效的防范手段。

1. 采用多种加密相结合的手段

例如我们写好一个Word文档，先利用Word自带的加密系统对该文档加密，然后将其压缩为一个加密的RAR文档，最后将这个RAR文档压缩为一个加密的ZIP文档。这样，如果要破解原始的Word文档，必须同时拥有三种不同的解密技术，客观上增加了破译难度。

2. 不要混用密码

不要用自己的邮箱密码、银行卡密码等重要密码作为文档加密的密码从前面介绍的Office密码暴力破解器，就可以看到破解Office文档的密码是如此简单和快捷。也许黑客很难获得你的银行卡密码，但是如果你用银行卡密码加密了一个Word文档并不幸将这个Word文档传播给黑客阅读，可以想象你将立即处于一个多么可怕的境地。

3. 使用高级的加密手法

可以使用数字加密、数字签名、公/私钥加密、证书等更为高级的加密方式。
高级加密和解密系统有很强的数学特性，这里仅做概念上的简要介绍。

在密码学中，经常提到公钥和私钥的概念。公钥是公开的密钥，即向网络中所有用户公开的一把电子钥匙。私钥是私有的电子钥匙，只有加密者自己知道。在一次从A到B的通信中，A和B相互知道对方的公钥。A使用B的公钥加密数据，B只有用自己的私钥才能解开这些加密数据，这就是所谓数字加密。A使用自己的私钥加密数据，则网络中包括B在内的所有用户都可以使用A公开的公钥解密数据，A不能抵赖自己已经发送的数据，这就是所谓数字签名。

数字加密（Digital Encryption）是研究利用数学算法将明文转变为不可能理解的密文，且反过来将密文转变为可理解形式的明文的方法、手段和理论的一门科学。要完成数字加密需要一种加密算法和一个密钥。加密算法其实就是一种数学函数，用来完成加密和解密运算。而密钥则由数字，字母组成，用它来实现对密文的加密或对密文的解密。相同的明文用不同的密钥加密得到不同的密文。数字加密的安全性取决于加密算法的强度和密钥的保密性。

数字签名（Digital Signature）是一种特殊的数字加密技术，它将数字加密的过程反向应用。在数字签名中，信息发送者使用公开密钥算法通过自己的私有密钥加密数据，产生别人无法伪造的一段数字串。接收者收到数据后，用发送者提供的公钥解开数据，就可确定消息的来源，同时也确定发送者发送信息的真实性。同时发送者对所发信息具有不可抵赖性。

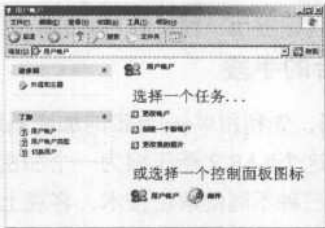
7.2.2 加密实例

下面介绍一些加密的实例，希望能对保护计算机信息安全有所帮助。

一、操作系统用户与密码

【案例7-16】操作系统用户与密码。

在计算机启动以后会在出现用户账户的对话框，一般情况下如果设置了多个用户账户的话。在Windows XP中，依次单击“开始”→“控制面板”→“用户账户”进入到用户账户的窗口，如图7-64所示。

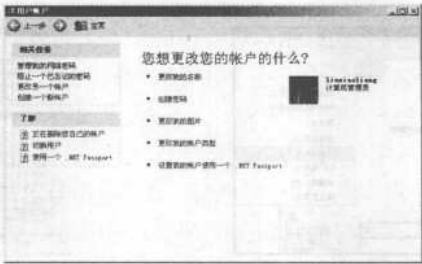


【图7-64】计算机系统用户密码设置

可以选择三个选项，分别是更改账户、创建一个新账户和更改我的图片，这里介绍和密码攻防有关的选项如下：

(1) 更改账户

进入到更改账户界面中，首先选择要更改的账户，然后进入到账户更改选择界面，如图7-65所示。



【图7-65】更改账户

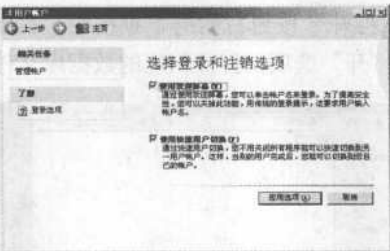
这个密码攻防有关的就是创建密码（没有设置密码，如果设置了密码该项是更改密码，以及多出一项删除密码）和更改用户类型。只要选择了相应的选项，按照提示来作即可完成相应操作，包括更改（创建密码）以及更改账户类型。

注意，只有是账户类型为系统用户的账户才能够创建新账户以及更改原有账户，受限后不能进行这些操作，包括对系统的其他修改。

(2) 创建一个新账户

当有其他人要使用该台计算机的时候可以创建一个新账户，可以创建为系统管理员账户或者受限账户，为了提供计算机的安全性，建议新创建账户是受限的。新创建的用户将会出现在欢迎屏幕和开始“菜单”中。

为了提供密码攻防的安全性，建议在“用户账户”中将登录的方式更改为传统的登录方式（这和Windows2000的登录方式相同），要求输入账户名和密码。在“用户账户”中选择打开“更改用户登录与注销的方式”窗口，将“使用欢迎屏幕”和“快速用户切换”复选项都取消选择即可。如图7-66所示。



【图7-66】“选择登录和注销选项”对话框

二、文档加密

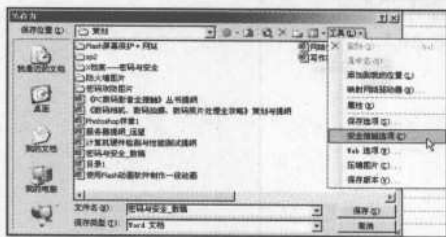
在工作过程中，很多重要的文档是要加密的，常见的就是Office文档以及Access数据库文



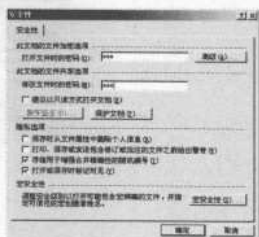
档了，但是很多人忽视了它的安全性。

【案例7-17】加密Office文档。

(1) 打开要进行加密的Word文档，通过菜单栏的“文件”→“另存为”打开另存为的对话框，然后选择“工具”→“安全措施选项”打开安全设置对话框，如图7-67和图7-68所示。



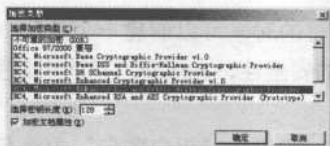
【图7-67】选择“安全措施选项”



【图7-68】“安全性”对话框

(2) 这里就可以为文档设置打开文档的密码以及修改文档的密码，确定后会要求再次输入打开以及修改文档密码，如果只有文档的密码就只能打开与阅读文档，不能修改保存文档，只有拥有了修改文档的密码才能做出修改。

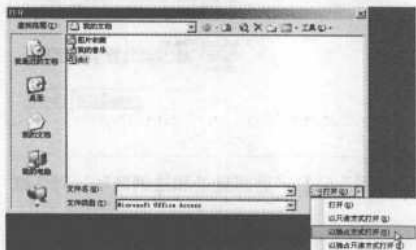
(3) 由于不同加密算法的密码安全性能不同，这里可以通过“高级”打开加密类型选择的对话框，如图7-69所示；一般情况下，建议选择RC4的RSA类型的加密算法，它具有良好的保密安全性能。



【图7-69】“加密类型”对话框

【案例7-18】加密Access数据库文档。

(1) 启动Access程序，执行“文件打开”命令，打开“打开”对话框，选中需要加密的数据库文件，然后按右下角“打开”按钮右侧的下拉按钮，在随后弹出的下拉列表中，如图7-70所示，选择“以独占方式打开”选项，打开相应的数据库文件。



【图7-70】选择“以独占方式打开”选项

(2) 执行“工具”→“安全”→“设置数据库密码”命令，打开“密码”对话框，如图7-72所示，设置好密码后，确定返回，即可对打开的数据库文件进行加密。



【图7-71】设置密码

三、网页加密

现在专业性的网站越来越多，许多个人都在网上建立起了自己的小家。不过辛辛苦苦制作的网页被别人拿去改头换面却是件非常痛心的事，所以大家都想保护自己原创性的作品，为自己的网页上把锁。有鉴于此，这里就来讨论如何为网页加把锁。

【案例7-19】JavaScript为网页加上密码锁。

JavaScript是一种新的网页描述语言，是由Sun公司以及网景（Netscape）公司开发的，这种语言可以被嵌入任何html的文件之中，使用它可以设计交互性很好的网页内容。使用javascript非常简单，只是插入一小段代码，就可以让网页产生千奇百怪的效果，而且使用javascript来加密的方法是网页加密最常用的。

使用javascript加密最简单的结果就是让浏览器不能使用鼠标右键，当点击右键想对图片进行保存或者复制文字的时候就会弹出一个警告窗口或弹出收藏夹对话框等。

(1) 利用弹出窗口封锁鼠标右键

将下面这段代码放在网页html代码的<head></head>标志中，就可以实现封锁右键，给网页加密。

```
<script language="javascript">
function click() {
if (event.button==2) {alert( '本站不准使用鼠标右键! ^_^' )}
}
document.onmousedown=click</script>
```

(2) 弹出“”添加收藏夹”对话框封锁鼠标右键

将下面这段代码放在网页的html代码的<head></head>标志中。实现点击右键出现“添加到收藏夹”对话框选项。

```
<script language="javascript">
function click() {
if (event.button==2) {window.external.addFavorite('http://www.uestc.edu.cn/','电子科大')}
}
document.onmousedown=click</script>
```

(3) 彻底封锁鼠标右键

将以下这段代码放在网页的HTML代码的<head></head>标志中能够实现彻底封锁鼠标

右键的效果，由于这个脚本在右键按下时调用一个函数，所以可以更改为很多种类型。即使按下左键，再按下右键，放开左键，再放开右键的方法也还是破解不了。

```
<script>
function DM(e){
if(!ns){
if(event.button>1)window.external.addFavorite('http://www.uestc.edu.cn/','电子科大')
else{if(e.which>1)
return false}
}
ns=navigator.appName=="Netscape";
if(ns)document.captureEvents(Event.MOUSEMOVE|Event.MOUSEDOWN);
document.onmousemove=DM;document.onmousedown=DM;</script>
```

(4) 禁止查看源文件

将下面这段代码放在网页的HTML代码的<head></head>标志中则可实现禁止利用IE浏览器来查看源文件。

```
<script language="JavaScript">
<!--
document.onmousedown=click
function click() {
if ( event.button==2) {alert('对不起，你无权查看本网页源文件！')}
if ( event.button==3) {alert('对不起，你无权查看本网页源文件！')}
}
//-->
</script>
```

(5) 用乱码显示链接、调用地址加密。

利用某些函数把URL字符转换成ASCII码，从而达到隐藏链接Frame页面以及*.js*.asp等源码脚本的目的。返回ASCII码escape(character)，ASCII码为%XX格式（XX是十六进制），如空格键为%20。返回字符unescape(string)

如：

```
<!--
var Words=" %3Cframeset%20BORDER%3D%22%22%20FRAMEBORDER%3D%22%22%
20FRAMESPACING%3D%22%22%20rows%3D%22100%25%22%3E%0D%0A%20%20%3Cframe
%20SRC%3D%22http%3A//XXX.XXX.COM/XXX/XXX/%22%20NAME%3D%22oos1%22%20"
//-->
</script>
```

利用javascript还可以使用调用脚本显示页面加密、密码校验等加密方法，但是由于代码繁杂以及使用难度较高而不经常使用，这里就不做过多讲述。

【案例7-20】使用IIS（Internet信息服务）的密码锁。

不要以为只有javascript可以加密网页，使用IIS也可实现类似的加密效果，只要计算机上安装的Web服务器是IIS，而使用者又是管理员权限的用户时，就可以用一种简单的方法来实现密码验证。

注意：这项操作要使用Win 2000/2003 Server版的操作系统，并且要安装了IIS及域用户管理器的组件。

1.启动IIS

- (1) 依次单击“开始”→“程序”→“Internet服务管理器”，打开“Internet 服务管理器”，展开左窗口的“网站”→“默认站点”，然后在展开的目录中选中加密的网页。
- (2) 然后单击“属性”按钮，打开“images属性”对话框，如图7-72所示。



【图7-72】“images属性”对话框

- (3) 接着选择“images属性”对话框中“目录安全性”标签，单击“匿名访问及验证控件”域中的“编辑”按钮，如图7-73所示。

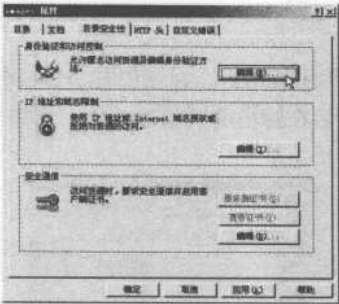


图7-73 “目录安全性”标签

- (4) 在弹出的“身份验证方法”对话框中，取消“启用匿名访问”选项前面的勾选，然后勾选“用户访问需经过身份验证”中的前三个选项，在弹出的提示对话框选择“是”并在“默认域”框中填写上默认的域控制器，最后单击“确定”按钮退出，如图7-74所示。



【图7-74】“身份验证方法”对话框

2.设置用户的名称及密码

只是对目录的安全进行设置还不行，为了让上网的用户只有在输入用户名称和密码后才可以浏览放在该目录下的网页，这里还要设置用户的名称及密码。

(1) 单击“开始”→“程序”→“管理工具”→“Active用户和计算机”，打开相应的窗口，如图7-75所示。



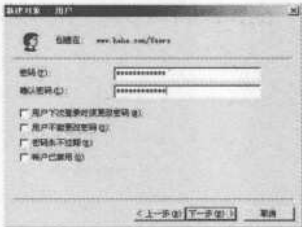
【图7-75】“Active用户和计算机”

(2) 在这里要给域用户里添加新用户，在窗口左边“Users”上单击右键，在弹出的菜单中选择“新建”→“用户”，然后在弹出的“新建对象-用户”窗口中输入新用户的信息，如图7-76所示。



【图7-76】“新建对象-用户”窗口

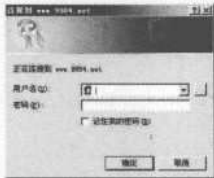
(3) 在下一步的窗口中输入用户密码以及取消“用户下次登录时须改变密码”的选项，如图7-77所示。



【图7-77】输入用户密码

(4) 一直单击“下一步”按钮完成新建用户。注意，新建用户必须设置好DNS和DHCP服务，以及满足相应的Windows安全策略的前提下。

(5) 到此为止，利用IIS服务器来给网页加密就全部完成了，当用户想访问安全目录下的网页时。只要在出现的要求输入网络用户名和密码的窗口中输入前面设置的新用户名及密码就可以进入安全设置目录，如图7-78所示。



【图7-78】登录IIS弹出窗口

【案例7-21】使用ASP程序密码锁。

除了使用IIS服务器来给网页加密，还可以使用ASP程序来给网页加密，一般来说利用程序来进行密码验证的方法比较通用，现在大多数网站都使用ASP程序，它对Web服务器没有具体要求，加密就是借助数据库及ASP程序进行设计，实现一种通用网页的加密操作。

(1) 打开Microsoft Access程序，建立一个“账号及密码”的数据表，假设将这个表取名为accounts，数据库名为iis.mdb，数据表的结构如下：

字段说明	字段名称	数据类型	数据长度
账号	ID	文本	15
密码	PWD	文本	15

(2) 编辑一个PASS.ASP的验证文件，源代码如下：

```
<%  
Function Check(ID, Pwd)  
Dim conn, par, rs  
Set conn = Server.CreateObject("ADODB.Connection")  
par="driver={Microsoft Access Driver (*.mdb)} "  
conn.Open par && ";dbq=" && Server.MapPath("iis.mdb")  
sql="Select ? From accounts Where ID=" && ID && " And Pwd = " && Pwd && ""
```

```
Set rs=conn.Execute(sql)
If rs.EOF Then
Check=False
Else
Check=True
End If
End Function
%>
<%
If IsEmpty(Session("Passed")) Then Session("Passed")=False
Head="请输入账号和密码"
ID=Request("ID")
Pwd=Request("Pwd")
If ID="" Or Pwd="" Then
Head="请输入账号和密码"
Else If Not Check(ID, Pwd) Then
Head="账号或密码有错"
Else
Session("Passed") = True
End If
If Not Session("Passed") Then
%>
<html>
<head> <title></title> </head>
<body BGCOLOR="#FFFFFF">
<h2 ALIGN="CENTER"><%=Head%></h2>
<hr WIDTH="100%">
<form Action="<%=Request.ServerVariables("PATH_INFO")%>" Method="POST">
<table BORDER="1" CELSPACING="0">
<tr>
<td ALIGN="RIGHT">账号: </td>
<td><input Type="Text" Name="ID" Size="12" Value="<%=ID%>"></td>
</tr>
<tr>
<td ALIGN="RIGHT">密码: </td>
<td><input Type="Password" Name="Pwd" Size="12" Value="<%=Pwd%>"></td>
</tr>
</table>
```

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

```
<p><input Type="Submit" Value="确定"> </p> </form>
<hr WIDTH="100%" align="center">
</body> </html>
<%Response.End
End If %>
```

(3) 在加密网页的HTML代码前面加上 “<! --#include file="pass.asp"-->” 就可以了。由于这个验证合法性的页面具有通用性，所以非常方便使用。

四、软件加密

通常情况下使用软件加密文件是最方便快捷的方法，而且安全性能也是非常高。加密软件种类繁多，使用的方法大同小异，都是根据一定的加密算法来对文件进行加密解密。

【案例7-22】使用万能加密器软件。

万能加密器具有加密文件大小不限、文件类型不限的特点；界面美观，有加/解密列表功能以及小巧易用的特性，具有很高的安全性。

(1) 万能加密器是一款免费绿色的软件，解压缩后无需安装即可使用，运行界面如图 7-79所示。



【图7-79】运行界面

(2) 只需要通过“添加文件”按钮将要加密的文件添加进加密列表中（可以添加多个文件），然后输入密码并确认，再单击“开始加密”按钮即开始加密。

(3) 加密后的文件不解密是不能打开的，例如加密后的Word文档，打开后将会是乱码而完全无法阅读。解密需要将文件添加到解密列表中（可以添加多个文件），然后输入正确的密码，单击解密按钮即可解密文件，如图7-80所示。



【图7-80】加密后的Word文档

(4) 直接进行加密后文件需要打开万能加密器来进行解密操作，这样会造成一定的麻



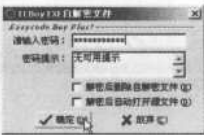
烦，如果使用“编译EXE”功能则可以解决这个问题，即使加密后没有万能加密器程序也可对加密文件进行解密，如图7-81所示。



【图7-81】使用“编译EXE”功能

(5) 选择要编译的文件，然后设置编译后的文件名，一般应该保持名称不便为好，这样便于以后查看文件；再来设置号加密密码并进行确认，然后单击“开始编译/加密”按钮即可开始操作。

(6) 在对上面加密的自解密EXE文件进行解密打开操作是会自动弹出一个对话框，要求输入解密密码，如图7-82所示。



【图7-82】输入解密密码

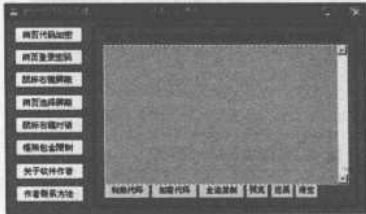
万能加密器还具有文件嵌入、分割以及伪装目录以及密码管理等等的功能，其实这些功能和上面提及的功能一样的简单实用，限于篇幅的原因这里不做过多讲述了。

【案例7-23】使用“世纪鸟网页加密精灵”加密网页。

“世纪鸟网页加密精灵”是一款绿色的小软件“世纪鸟网页加密精灵”，能更方便快速地对网页加密。

使用“世纪鸟网页加密精灵”的“网页登录密码”选项来给网页加密，具体步骤如下：

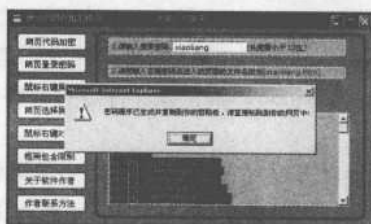
(1) 打开要加密的网页，复制出HTML源代码，然后打开“世纪鸟网页加密精灵”软件，选择“网页登录密码”选项，这时在右边就会出现一些输入框内的代码说明，如图7-83所示。



【图7-83】打开“世纪鸟网页加密精灵”软件

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(2) 在“请输入登录密码”的输入框中输入长度小于10位的密码，然后单击“生成并复制密码页面程序”按钮，这时软件会自动在下方的javascript代码中加入要输入的登录密码作为验证信息，并将这段代码复制到你的剪贴版中，如图7-84所示。



【图7-84】“请输入登录密码”的输入框

(3) 接下来再将这段代码粘贴到网页中,并将网页改名为(你输入的登录密码).htm,这样就可以对此文件加密了。

7.3 系统EFS加密解密

远离自己的计算机，如何有效地保护计算机上文件的安全呢？在微软操作系统基础上有一种很好的解决方案是：如果把这些文件加密，没有正确的密码，别人就不能正确读取这些文件。即使获得这些文件，也是没有任何意义的。Windows 2000 Professional 和 Windows XP Professional，包括Windows Vista都提供了一种文件加密系统，即文件系统（Encrypting File System，简称：EFS）。

7.3.1 EFS简单介绍

EFS (encrypting file system, 文件加密系统): 它主要提供一种核心文件加密技术, 对 NTFS 文件系统卷上存储已加密的文件

NTFS 文件系统介绍：它比FAT版本提供了更安全、可靠性的服务，比如，NTFS 通过使用标准的事务处理记录和还原技术来保证卷的一致性。如果系统出现故障，NTFS 将使用日志文件和检查点信息来恢复文件系统的一致性。NTFS 还可以提供诸如文件和文件夹权限、加密、磁盘配额和压缩之类的高级功能。

1.什么是加密文件系统EFS

加密文件系统 (EFS) 是 Windows 2000、Windows XP Professional、Windows Server 2003 及 Windows Vista 的 NTFS 文件系统的一个组件 (Windows XP Home 不包含 EFS。) EFS 采用高级的标准加密算法实现透明的文件加密和解密, 任何不拥有合适密钥的个人或者程序都不能读取加密数据。即便是物理拥有驻留加密文件的计算机, 加密文件仍然受到保护, 甚至是有权访问计算机及其文件系统的用户, 也无法读取这些数据。

EFS的工作原理

当使用EFS时，对于每个加密过的文件或文件夹都会得到一个唯一的加密密钥的保护，该密钥受到用户凭证的保护，从而确保任何其他人员都无权访问这些文件——除非他们的凭证可以解开这些文件/文件夹的特定密钥，否则无法读取。该文件在磁盘上一直处于加密状态；授权用户可以复制或移动这个采用加密形式的文件。当授权用户尝试打开该文件时，Windows就自动在内存中对其进行解密，并且将每个加密的数据块传送到请求应用程序中；Windows决不会将未经加密的数据写入磁盘。在Windows解密该文件或将其移到一个未加密的文件夹之前，它会一直处于加密状态。

许多企业都会对业务持续性和系统访问感到担忧——如果你雇用的员工加密了一些数据而后又离职了，会发生什么事呢？这种担忧是有道理的，因为EFS采用的加密算法与银行用来保护ATM交易的算法是一样的。EFS支持恢复代理，恢复代理可以获取加密项的所有权并且对其进行解密。一旦恢复代理恢复了加密文件，原始的拥有者就可能会泄密，因为文件不再处于加密状态。这种机制可以防止一些好事的恢复代理对保密数据进行未经授权的操作。

Windows XP Professional将一些非常好的特征添加到Windows 2000的EFS中。而重要的是，它可以允许其他用户使用别人的加密文件。这样就在EFS的安全性和共享数据的便利性之间建立了良好的平衡。Windows XP EFS允许加密Web文件夹和脱机文件夹中的文件，这意味着在共享和传输保密数据的同时，不放弃安全性。

2. 加密文件系统EFS的作用及应用条件

了解了加密文件EFS的原理后，来看看它的作用。当用户一旦使用EFS对存储在硬盘上的文件加密后，EFS便开始起作用。它的作用就是让用户对计算机文件系统中的文件进行加密，EFS并没有设计成可以保护从一个系统传送到另一个系统的数据，它采用的是对称（使用一个密钥来加密文件）和非对称（使用两个密钥来保护加密密钥）加密。

应用条件：当你使用了Windows 2000/XP/2003/Vista系统（注意Windows XP家庭版不支持EFS加密文件系统），且格式化磁盘为NTFS文件系统，就拥有了应用EFS的条件。

使用加密文件和文件夹时的注意事项：

（1）只有NTFS卷上的文件或文件夹才能被加密。由于WebDAV使用NTFS，当通过WebDAV（Web分布式创作和版本控制）加密文件时需用NTFS。

（2）不能加密压缩的文件或文件夹。如果用户加密某个压缩文件或文件夹，则该文件或文件夹将会被解压。如果将加密的文件复制或移动到非NTFS格式的卷上，该文件将会被解密。如果将非加密文件移动到加密文件夹中，则这些文件将在新文件夹中自动加密。然而，反向操作则不能自动解密文件。文件必须明确解密，除非移动到非NTFS的卷上。

（3）无法加密标记为“系统”属性的文件，且位于%systemroot%目录结构中的文件也无法加密。

（4）在允许进行远程加密的远程计算机上可以加密或解密文件及文件夹。然而，如果通过网络打开已加密文件，通过此过程在网络上传输的数据并未加密。必须使用诸如SSL/TLS（安全套接字层/传输层安全性）或Internet协议安全性（IPSec）等其他协议通过有线加密数据。

3. 什么是数字证书

数字证书，它的英文是“Digital ID”。数字证书提供了一种在Internet上身份验证的方

式，是用来标识和证明通信双方身份的数字信息文件，其功能与司机的驾照和日常生活中的身份证相似。在网上进行电子商务活动时，交易双方需要使用数字证书来表明自己的身份，并使用数字证书来进行有关交易操作。通俗地讲，数字证书就是个人或单位在Internet上的身份证，它由认证权威含机构（CA），例如“VeriSign,Inc.”对某个拥有者的公钥进行核实之后发布，数字证书是由CA进行数字签名的公钥，证书通过加密的邮件发送以证明发信人确实和自己宣称的身份一致。

7.3.2 用EFS加密文件

当你使用了Windows 2000/XP/2003系统（注意Windows XP家庭版不支持EFS加密文件系统），且格式化磁盘为NTFS文件系统，你就具有了应用EFS的条件。

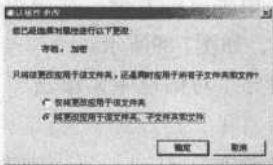
【案例7-24】使用EFS加密。

(1) 要使用EFS加密，只须打开资源管理器，在需要加密的文件（夹）上点鼠标右键，选“属性”，在“属性”对话框中点“高级”打开“高级属性”对话框，勾选“加密内容以便保护数据”（取消该选项前的钩即可解密文件），然后“确定”按钮，如图7-85所示。



【图7-85】“高级属性”对话框

(2) 在弹出的“确认属性更改”对话框中单击“应用”按钮，如果加密的是文件夹，则会弹出如图7-86所示对话框，你可以根据需要选择是仅加密此文件夹还是将此文件夹下的子文件夹和文件也一起加密。



【图7-86】“确认属性更改”对话框

(3) 最后单击“确定”按钮，在默认情况下，文件（夹）在资源管理器中显示的颜色变为彩色，表示已经被加密（或压缩）了。

注意：你也可以不使文件（夹）变色，在资源管理器中，依次单击“工具”→“文件夹选项”→“查看”，将“用彩色显示加密或压缩的NTFS文件”取消即可。

7.3.3 备份加密证书

既然EFS采用加密密钥来加解密，那么只要加密密钥存在，就能恢复数据。因此，将密钥备份下来以作不时之需是最好的办法。

当系统发生问题或崩溃时，被加密过的文件夹或文件怎么办？通常情况下，加过密的EFS文件在没有备份密钥的情况下，解密是比较麻烦的。因为某些EFS使用的是公钥证书对文件加密，而且在Windows 2000/XP中，每一个用户都使用了惟一的SID（安全标志）。如果在重装系统之前没有对当前的密钥备份，那就意味着无论如何都不可能生成此前的用户密钥，而解密文件不仅需要公钥，还需要密码，所以也就根本不能打开此前EFS加密过的文件夹。

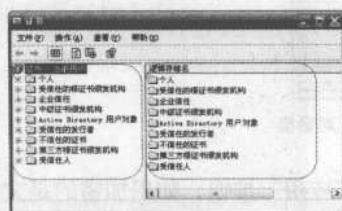
因此，在EFS加密后进行证书的备份显得尤为重要。

『案例7-25』在Windows系统中备份加密证书。

在Windows2000/XP/2003中备份加密证书和私钥的方法大致相同，现在以Windows X P下备份加密证书和私钥为例，具体操作步骤如下。

(1) 选择“开始”→“运行”命令，在弹出的“运行”对话框中输入“certmgr.msc”，打开证书管理器主界面，如图7-87所示。

(2) 选择“证书”目录下的“个人”，展开“个人”文件夹，如果做过加密操作，右边窗口就会有与用户名同名的证书，如darcy，如图7-88所示。



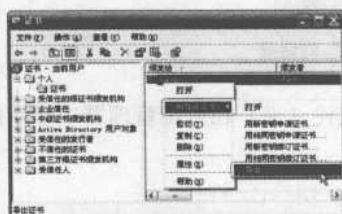
【图7-87】证书主界面



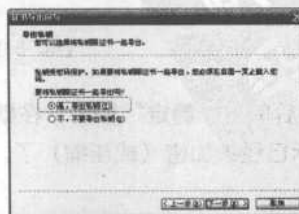
【图7-88】个人证书

(3) 选中“darcy”证书后，单击鼠标右键，在弹出的快捷菜单中选择“所有任务→导出”，这将启动“证书导出向导”，如图7-89所示。

(4) 在弹出的“证书导出向导”对话框中，单击“下一步”按钮，选择“是，导出私钥”复选框。如图7-90所示。



【图7-89】导出证书

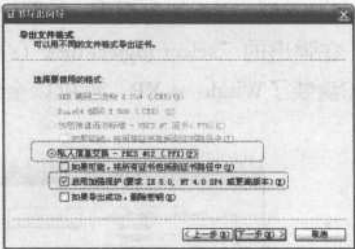


【图7-90】证书导出向导

(5) 再单击“下一步”按钮，弹出“导出文件格式”对话框，选择“私人信息交

换-PKCS #12 (.PFX) (P)”中的“启用加强保护（要求IE5.0，NT4.0 SP4或更高版本）（E）”复选框，如图7-91所示。

(6) 单击“下一步”按钮，弹出“密码”对话框，输入“密码”并进行确认以保护导出的证书，如图7-92所示。



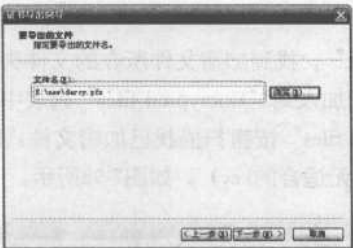
【图7-91】导出文件格式



【图7-92】密码对话框

(7) 单击“下一步”按钮，弹出“要导出的文件”对话框，可以在“文件名”文本框中输入要保存的位置及文件名，文件的扩展名是.pfx，或通过“浏览”按钮来选择一个位置及文件名，如图7-93所示。

(8) 单击“下一步”按钮，弹出“正在完成证书导出向导”对话框，显示出刚才所保存的文件的位置及有关证书的相关信息，如图7-94所示。



【图7-93】指定导出的文件名



【图7-94】完成证书导出向导

(9) 单击“完成”按钮，到此，证书成功导出。

7.3.4 解密用EFS加密的文件

对文件采用EFS加密后，系统无法启动或崩溃等，如果没有备份密钥，硬盘上EFS加密的文件便无法打开。这时可以采用另一种方法，那就是专门针对EFS加密文件的解密软件，在本节，将介绍几款比较常用的解密EFS软件。

【案例7-26】：利用Advanced EFS Data Recovery解密EFS加密文件。

1. 软件介绍

Advanced EFS Data Recovery简称AEFSDR，它主要能完成NTFS分区里解密EFS加密的解密

任务，即使系统不能够启动，不能登录进去，AEFSDR也能有效地破解EFS加密的文件，它支持 Windows 2000，Windows XP，Windows Server 2003 及 Windows Vista，甚至可以恢复密码钥匙。

2. 解密EFS

具体的操作步骤如下：

- (1) 运行Advanced EFS Data Recovery，进入Advanced EFS Data Recovery界面，如图7-95所示。
- (2) 单击“Scan for keys”按钮，扫描查找keys，在弹出的“select logical disk (s) to scan”对话框中选中选择有操作系统的磁盘分区，如只有C盘装了Windows XP，也可以全部选上，不过扫描时间会长些，如图7-96所示。



【图7-95】Advanced EFS Data Recovery主界面



【图7-96】选择逻辑扫描盘

- (3) 选好分区，单击“Start Scan”按钮。程序会自动在各分区中搜索key，有效的key会用绿色显示在列表中，如图7-97所示。
- (4) 找出需要解密的文件：单击界面的“File tree”，找到加密文件所在的文件夹，在右侧单击文件，选择“Add files (s) into list”按钮，把它们加入到“Encrypted files”列表中，也可以在“Encrypted files”界面中，使用“Scan for encrypted files”按钮扫描找已加密文件。Encrypted files列表中绿色的文件表示可以破解，红的不能破解（无适合的key）。如图7-98所示。



【图7-97】扫描结果



【图7-98】扫描加密的文件

- (5) 在“Encrypted files”列表选中需要解密的文件，选好后单击“Decrypt”按钮。在弹出的对话框（select folder where decrypted files will be written）选择破解文件写入的路径，单击“确定”按钮，系统会自动破解，其间显示保存已破解文件进度，破解完成后显示破解成功提示，如图7-99所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图7-99】选择破译的文件

(6) 破解后的文件存放在你所指定的磁盘的“\AEFSDR_E_DECRYPTED”目录下，文件数，大小与原文件夹下一样，只是文件名与原来不同。



在使用Advanced EFS Data Recovery英文版时，对中文文件名支持不太好，最好使用英文或数字文件名。

【案例7-27】：EFSKey解密EFS加密文件。

1. 软件介绍

EFSKey主要是磁盘格式加密文件恢复工具，它不需要用户接触技术细节，复原文件完全是透明进行的。

2. 解密EFS

它的使用很简单，具体操作步骤如下。

(1) 运行EFSKey程序。

(2) 在EFSKey 主界面，有点类似资源管理器，通过浏览，选择要解密的文件，程序会自动寻找加密密钥解码，和Advanced EFS data recovery相似，不能解码的文件图示会显示红色锁匙，能解码的图示会标示为绿色锁匙，如图7-100所示。



【图7-100】EFSKey解密文件

【案例7-28】：PsExec 和IceSword的方法破解EFS加密文件。

1. 软件介绍

PsExec是一个小型的telnet替代工具，使用它需手动安装客户端软件才能执行其他系统上的进程，并且可以获得与控制台应用程序相当的完全交互性。PsExec 最强大的功能之一是在远程系统中启动交互式命令提示窗口，以便显示无法通过其他方式显示的有关远程系统的信息。

IceSword是斩断黑手的利刃，用于查探系统中的幕后黑手-木马后门，并作出处理。

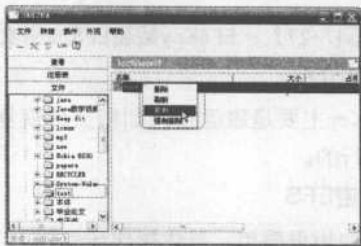
2. 恢复EFS文件

利用PsExec和IceSword结合起来恢复EFS文件，以在Windows XP系统中NTFS磁盘上的E盘建立一个test文件夹为例，启用EFS加密。文件夹中有一个加密过的文本文件test.txt，系统中有两个用户，系统管理员darcy和test，darcy属于administrators组，test属于users组，具体操作步骤如下。

- (1) 用系统管理员darcy登录，在NTFS磁盘上的E盘建立一个test文件夹，并建立一个test.txt文件。
- (2) 注销计算机，启用test 用户登录，打开cmd，在任务管理器中终止explorer.exe进程，打开PsExec尝试用system登录，在CMD中输入如下命令：PsExec -i -s -d explorer，再打开test.txt文件，为乱码，如图7-101所示。
- (3) 运行IceSword.exe，选择“文件”项，浏览test文件夹，右键选择test.txt，在弹出的快捷菜单中，选择“复制”项，复制到桌面，文件名任意，后缀不变，如图7-102所示。



【图7-101】cmd命令行



【图7-102】IceSword 界面

- (4) 在桌面双击打开文件，成功读出。



本方法适用的条件为：在系统内还有该EFS加密文件相对应的密钥，否则也不能成功恢复。

7.4 小结

本章介绍了多种密码破解工具及其用法。读者阅读本章之后，应该具备使用这些工具对目前各种流行的文件加密和解密的能力。本章最后对如何防范密码破译工具给出了一些方法。

破解与反破解永远是道高一尺，魔高一丈的争斗。软件想要成功，除了在软件中加强保护的力度，还需要不断提高编程者的水准，才能做出高质量，有独特的创新，能真正满足用户需要的软件。

第8章

共享软件的加解密工具

在计算机飞速发展的今天,软件的更新速度也越来越快。在推出新产品的同时,网络上也不断在推出更新软件的破解版本。世界上破解组织越来越快的破解速度,给软件企业和软件作者带来比较大的压力。这些组织是如何破解软件,企业又是如何保护软件的呢?

本章要点

- ◎ 软件加密及解密基础
- ◎ 共享软件加密
- ◎ 共享软件解密

8.1 软件的加密及解密基础

在计算机飞速发展的今天,软件的更新速度也越来越快。在推出新产品的同时,网络上也不断在推出软件的破解版本。世界上破解组织越来越快的破解速度,给软件企业和软件作者带来比较大的压力。这些组织是如何破解软件,企业又是如何保护软件的呢?

8.1.1 软件的加密技术基础

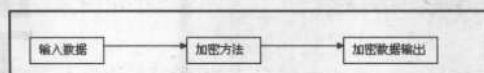
软件销售最重要的是保护软件,软件加密的好坏直接关系着软件以后的发展。软件加密是密码学的一个重要应用。在计算机、军事、经济、银行等领域对信息保密的要求越来越高,把相应的加密文件还原就是解密的过程。研究信息更难被破解的加密方法,就是密码学。

加密有很多种方法,下面介绍两种常用的:

代码法,既是明文中用到所有词组成集合为M,密码字符或数字为N,它们之间是一一对应关系。加密解密就是这种对应关系编制的加密解密软件,但是这种加密方法效率非常低,在计算机上破解时,会占用大量的资源。在实际的加密解密中,很少应用的这种破解方法。

密码法,包括置换法、代替法、乘积密码法等多种方法:置换法是将明文即原文件的字母顺序进行重新排列,从而加密原文件;代替法,是将明文中的字符或字母用另外一个字母或字符替代的方法;乘积密码法,则是保密性比较高的一种方法。通过混合置换法和代替法的方法达到使明文很难破解。

加密系统模型是一个信息系统处理模型,明文加密处理过程。加密系统中输入数据为明文,加密数据输出为密文,加密的关键是加密的方法。



密码从根本上说都是代替密码。在明文加密过程中,给定明文信息一个密钥,经过加密过程变成唯一的密文信息,就是明文和密文之间的替换。在软件的序列号加密算法的编写中可以采用密码学的算法,RSA、MD5、SHA、N-Hash、HAVAL等算法可以在网上下载编译好的源文件或库。用户可以直接利用并写入自己的程序中。这些密码学的算法强度比较大,不容易被破解。文件在光盘上以二进制数据文件和ASCII代码保存。二进制文件可采用反汇编的方式进行阅读,保密性比较好,破译比较困难。高级语言和软件应用包编写的源程序文件存储格式为ASCII码文件,可读性比较强。为防止程序被破解,软件需要加密。

软件加密就是通常的加壳,壳专门保护软件不被修改或反编译的程序,先于软件运行,拿到软件控制权进而保护软件。现在加密的软件比较多,一些软件增加了压缩的功能,把文件压缩以后,再加上一层在软件被执行的时候自动解压缩文件的壳来压缩文件。一般在软件编写完成后,都需要对软件加壳,一方面减少软件的大小,另一方面保护软件不被修改或破解。压缩加壳的软件的EXE文件是可执行文件,这种文件同正常的文件一样可以执行,实际上用户执行的是外壳程序。当运行程序时,壳负责把程序在内存中解压,程序是在内存中运行的,用户

感觉不到程序的变化。加壳减少了程序在内存中的加载，抵消了程序运行壳的时间，所以运行速度变化不大。

软件加壳起到了保护软件的作用，在实际中软件厂家广泛使用。加壳软件层出不穷，各个软件都有自己的加壳特色，如何更好地加密软件是成为软件厂商共同的目标。

8.1.2 软件的解密技术基础

软件解密的发展随着加密的发展而发展，网络把世界各个国家的解密高手联系到了一起，只要有新的软件产品发布，不久就会有新的破解版本出来。这些破解组织分工明确，专门的部门负责购买、破解、发布软件。有时解密软件发布甚至超过了软件厂家新软件的发布，给软件厂家带了巨大的损失。随着加壳工具的发展，脱壳工具也在不断发展。在熟悉软件破解基本技术，才可更好地解密软件。这里介绍软件的解密，主要让大家认识一些软件方面的技术，更好地提高软件保护意识，不要用在非法途径。

在软件解密之前，我们首先要对软件脱壳，软件脱壳的方法主要有自动脱壳和手动脱壳两种。

自动脱壳是通过软件自动脱去软件加上的外壳。在脱壳之前，要检测软件是否加壳，加什么壳。FileInfo、GetTyp、TYP是比较有名的探测文件类型工具，能检测多种文件格式，脱壳之前用来判断是否加壳或何种壳。探测软件完成后，就可以使用脱壳工具对软件脱壳。一般某种压缩工具的壳，都会有相应的脱壳工具。找到相应的新版本脱壳工具，可以容易地脱去。ASPack unpaccker是脱ASPack的压缩PE文件；UnPEpack是脱Pepack的壳的工具；ProcDump32是一款优秀的“万能”脱壳工具，可以脱去老版本压缩工具的壳，可惜不能升级。手动脱壳是不借助自动脱壳工具，利用动态调试工具SOFTICE或TRW2000来脱壳，先熟悉一些基本的原理，为以后深入研究做铺垫。

(1) 探测软件，用FileInfo、GetTyp、TYP等软件探测软件是何种壳。

(2) 确定入口点，入口点的查找比较难，但是熟悉之后，查找起来就比较容易，看到一个跨越段的JMP就有可能是入口点，因为多数PE加壳程序在被加密程序中加上一个或多个段，PE文件为Microsoft设计的一种新的文件格式Portable Executable File Format(即PE格式)，应用于所有基于Win32的系统，另外用冲击波2000,也能轻易地找到加密壳的入口点。

(3) 用Prodump取内存已还原文件，找到入点后，用软件Prodump的FULL DUMP功能来抓取内存中的文件，也可以用TRW2000的makepe和pedump命令实现功能；

(4) 修正Prodump取出的文件，假如是用Prodump的FULL DUMP功能脱壳的文件，需要用Procdump或PEditor等PE编辑工具修正入口点。

在软件脱壳后，就可以对软件进行解密。软件的破解主要两种，一是补丁，编写小程序实现对软件内部某种特定程序的改变，通常只是针对一个版本，注意使用的版本要和补丁一致，如果不一致，可能导致程序破坏；二是注册码，使用注册码比较安全，一般情况下不会对计算机造成伤害。在写注册机的时候，要通过一定算法推出注册码的程序，要了解注册码的算法，使用高级语言或汇编语言还原算法。有了注册机大家就可以方便地使用软件。

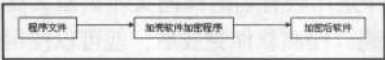
补丁的制作比较简单，可以使用CodeFusion软件制作，软件可以自动比较补丁前后差别，前后文件的大小，可以处理不同盘、不同目录等多项功能。另外，也可以使用RPP.EXE制作内存动态补丁，通过脚本命令创建win32文件，按脚本要求修补内存中的指令实现软件的内存动态补丁。注册机的制作比较复杂，因为写注册机之前，要了解程式的算法，然后用汇编语言等编写出程序，花费的时间比较长。可以使用CrackCode2000，制作一个注册机，但是软件的应用是有限的。

软件的破解技术比较复杂，需要更多的实践。在实践中不断的积累，才可以熟练地掌握软件破解。

8.1.3 软件加密解密流程

软件的加密技术主要是软件实现保护的技术，一方面可以在软件源文件中加入注册码等技术实现对软件的加密，另一方面是对软件加壳，这里主要向大家介绍软件加壳保护软件。

软件加壳的过程比较简单，输入为程序编译文件，输出为加密后软件，处理过程为加壳软件加密程序。各个加壳软件的功能不同，软件实现的加密效果不同，加壳软件的选择非常重要，直接关系着保护软件效果。



在网上软件破解是比较热门的话题，可以破解软件是一个人网络知识的证明，因为真正的软件破解比软件加密要难。软件解密的步骤一般为：

- (1) 探测软件是否加壳，采用的什么软件加壳。
- (2) 如果软件加壳，采用相应的软件脱壳。
- (3) 查看软件源文件，并查找关键字。
- (4) 破解软件。



掌握软件加密解密需要在实践中不断积累，大多数软件的加密和解密流程是一样。在掌握软件基本破解的基础上，可对软件加密和解密进行深入研究。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图8-3】软件探测结果显示



【图8-4】ASPACK软件界面

(5) 单击“Open”按钮，弹出select file to compress（选择压缩文件）对话框，如图8-5所示。选择需要加壳文件“hgh棋.exe”，然后再单击“打开”按钮。



【图8-5】选择压缩文件对话框

(6) ASPACK开始压缩软件，压缩后软件的占用空间变小。启动压缩后的软件，发现和压缩前没有大的区别。也可以采用其他加壳软件对软件加密，保护共享软件，如图8-6所示。



【图8-6】ASPACK压缩软件

8.2.2添加反跟踪保护共享软件

软件发布要和软件的保护紧密结合起来，好的软件需要有更好的保护。如果没有反跟踪技术，软件就等于直接裸露在外。反跟踪技术主要包括防静态反汇编、防调试、防监视等，反跟踪可以更好地保护软件，使软件不被破解。

软件的编写可以采用相关的代码和技术，增强软件的保护，下面介绍一些针对破解工具常用的反跟踪方法。

1.Anti-Debug

(1) MeltICE子类型

类型：检测SoftICE、TRW2000

平台：Windows9x、Windows NT

原理：用CreateFileA（）或_lopen（）函数试图获得SoftICE的驱动程序“\\.\SICE”（Windows9X版本）、“\\.\SIWDEBUG”、“\\.\NTICE”（Windows NT版本）、“\\.\

SIWVID" 等的句柄，如果成功则说明SoftICE驻留在内存中。

(2) DevIO—ConnectToSoftICE子类型

类型：检测SoftICE

平台：windows 9x、Windows NT

原理：利用 SoftICE白带的Nmtans.dll中的DevIO—ConnectToSoftICE () 判断SoftICE是否驻留。

(3) BoundsChecker后门

类型：检测SoftICE

平台：Windows9x、Windows NT

原理：这是SoftICE为BoundsChecker留的一个公开的接口，入口参数EBP = 0x4243484B (即"BCHK")，AL = 4，如果SoftICE在内存中则应返回AL = 0。

(4) VWIN32_Int41Dispatch子类型

类型：检测SoftICE

平台：Windows9x

原理：VWIN32.VxD (其VxD ID为0x002A) 提供一个名为VWIN32_Int41Dispatch的VxD service (其service ID为0x002A)，系统内核使用此服务来与系统级调试器如WinDBG、SoftICE等进行通信。其中0x4F号子功能是用来查询调试器是否已经驻留内存并能否处理保护模式程序，如果是的话调试器应返回0xF386。

(5) IsDebuggerPresent子类型

类型：检测SoftICE

平台：Windows NT

原理：调用kernel32.dll输出的函数IsDebuggerPresent () 来检测是否有调试器存在。这个函数只能检查使用Debug API来跟踪程序的调试器，无法检测SoftICE之类的系统级调试器。

(6) ICECream子类型

类型：检测SoftICE、TRW2000

平台：Windows9x

原理：调试器驻留后修改INT 1和INT 3的入口，指向它自己的处理程序，所以入口高位偏移与其他中断不同。其他所有中断入口高位偏移都相同。

(7) 注册表键

类型：检测SoftICE配。

平台：Windows 9x和Windows NT。

原理：即检查注册表中的键HKEY_LOCAL—MACHINE\SOFTWARE\NuMega及其相应的子键。这种方法实用性不大，因为无法据此确定SoftICE是否驻留在内存中。

(8) CMPXCHG8B子类型

类型：检测SoftICE。

平台：Windows 9x、Windows NT。

原理：使用指令的一种非法形式CMPXCHG8B (LOCK前缀)，检测SoftICE并且使其。机

器码为FO OF C7 C8。

2.CRC介绍

软件的加密可以通过检查程序的完整性，或者代码的完整性，防止程序被修改，进而达到防止软件被破解。检查完整性的算法比较多，例如MD5、SHA等单向散列算法，比较常用的CRC算法包括CRC16和CRC32。

算法检查一般是把程序的一部分或全部计算出一个值，用这个值和预期的值比较。如果不一致，有可能出现病毒或计算机程序被破解，程序在这种情况下就会终止运行。

3.Anti-W32Dasm

(1) 死循环语句

类型：对付W32Dasm

平台：Windows 9x和Windows NT

原理：下面是故意在程序中插入的一个死循环，可能会使W32Dasm的某些版本停止响应。

对策：W32Dasm进入死循环后，用bpx hmempcy设置断点，来到死循环代码处，将其跳出死循环，或用IDA反汇编。

(2) 花指令

解密者经常用反汇编工具对软件进行分析进而破解软件，优秀的汇编软件可以很好地区分软件中的程序和指令，一些软件增加了干扰反汇编的技术。常用的一种方法是花指令，包括利用一些无用的字节干扰反汇编的程序，创建一个陷阱。

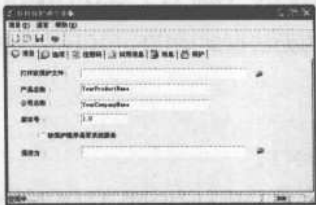
当反汇编发生错误时，反汇编软件错误地确定了指令的起始位置，导致反汇编一些跳转指令跳转的位置无效，具有这样特征的程序，可以确定该程序中使用了花指令。

另外，Anti-Dump、SEH技术、Anti-RegMon和FileMon等反跟踪技术的使用增加了软件的安全性。反跟踪技术加强了对软件的保护，增加了对软件的破解难度。

【案例8-2】利用软件保护神进行软件反跟踪。

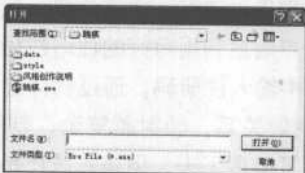
软件增加反跟踪技术也可以通过软件添加。软件保护神就是一款非常优秀的软件，使用最新的反跟踪技术，并增加独创的反跟踪技术，可以让软件拥有代码变形、花指令、反跟踪、反汇编、反转储（antidump）、反内存补丁、反API钩子、文件完整性检查等功能，具体的操作步骤如下：

(1) 首先启动软件保护神，进入主界面，主界面包括：项目、选项、注册码、试用信息、消息、保护六个选项卡，这也是增加软件保护的流程，如图8-7所示。



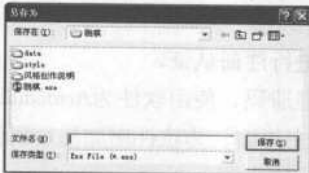
【图8-7】软件保护神界面

(2) 单击“项目”选项卡，并单击“打开欲保护文件文本框”后按钮，弹出“打开”对话框，如图8-8所示。选中准备添加反跟踪并加壳软件，例如选中跳棋文件，单击“打开”按钮。输入产品名称、公司名称、版本号等。



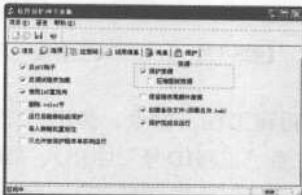
【图8-8】打开对话框

(3) 单击“保存为文本框”后的按钮，弹出“另存为”对话框，选择文件保存位置并输入文件名，这里保存添加反跟踪后的软件，单击“保存”按钮，如图8-9所示。



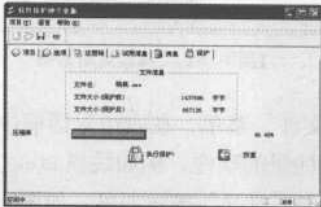
【图8-9】另存为对话框

(4) 返回软件保护神主界面，选择“选项”选项卡，这里是软件添加反跟踪的关键。选择“反API钩子”、“反调试程序加载”和“使用IAI重定向”，其他的选项可以根据需要选择，如图8-10所示。



【图8-10】“选项”选项卡

(5) “注册码”、“试用信息”、“消息”选项卡采用默认设置。单击“保护”选项卡，单击“执行保护”按钮，开始压缩软件并添加反跟踪保护，执行完成显示文件信息，可以查看文件保护前和保护后的大小，如图8-11所示。



【图8-11】保护选项卡

8.2.3 增加注册认证保护共享软件

增加注册认证是软件保护的一项重要措施。通常软件是在使用日期上，或者在使用功能上进行限制。这样可以保护软件不容易被破解。软件注册一般是用户把自己的个人信息和注册费用发送到软件公司，公司根据用户信息利用写好的注册码程序算出一个序列号，通过电子邮件等形式发送给用户。用户在软件中输入注册码，通过软件验证后，软件的各种限制被取消。

用户名和注册码之间是一种映射关系，映射越复杂，软件越难破解。现在很多序列号算法是软件作者自行开发的，虽然下了很多工夫，但是算法还是比较简单，容易被破解。软件注册可以借用密码学的算法，例如，RSA、Blowfish、MD5等，这些算法可以在网络上下载，算法强度比较高，不容易破解。

软件注册一种是在软件代码中增加注册算法，另一种是软件编译完成后，利用软件增加注册。

【案例8-3】利用Armadillo进行注册认证。

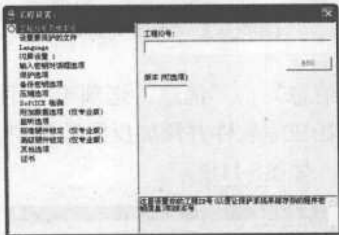
下面介绍如何使用软件增加注册码，使用软件为Armadillo 4.4，具体的操作步骤如下：

- (1) 首先启动进入Armadillo主界面，为软件增加注册码保护，如图8-12所示。



【图8-12】Armadillo主界面

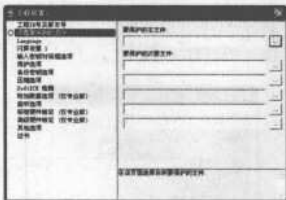
- (2) 单击执行“文件”→“新建工程”命令，弹出“工程设置”对话框。然后展开“工程ID号及版本号”菜单，在软件右侧“工程ID号”中出入“跳棋”，如图8-13所示。



【图8-13】工程设置对话框

- (3) 展开“设置要保护的文件”菜单，在右边对话框中单击“要保护的主文件”按钮，弹出“打开”对话框，选中添加注册的软件，例如跳棋.exe。假如还有其他的Dll文件，可在要保护的次要文件中逐一添加，单击“打开”按钮即可，如图8-14所示。

第8章 共享软件的加解密工具



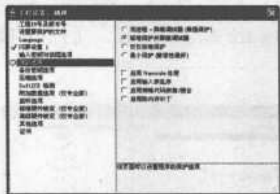
【图8-14】设置要保护的文件界面

(4) 展开“闪屏设置1”菜单，设置启动软件时的信息框。“无闪屏窗口”是不显示任何信息；“显示默认值”是显示默认信息窗口，出现加载进度；“显示Bitmap图片”是显示图片，可定义背景信息图，如图8-15所示。



【图8-15】闪屏设置1界面

(5) 展开“保护选项”菜单，设置软件保护。该对话框给出了“双进程+屏蔽调试器（最强保护）”、“标准保护并屏蔽调试器”和“仅仅标准保护”等多个选择，可以根据需要选择，这里选择“标准保护并屏蔽调试器”，如图8-16所示。



【图8-16】保护选项界面

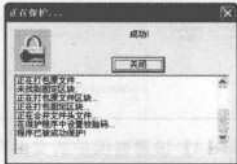
(6) 展开“证书”菜单，在证书界面中单击“新建”按钮，弹出“证书”设置对话框，输入“证书的名字”和“密码模板”，选中“使用Digital River版本密钥”。在签名等级选中“等级10”，并选择“Allow Key Strings (Pro)”，如图8-17所示。单击“硬件锁定（仅专业版）”，选中“标准硬件锁定”。关闭证书设置对话框和工程设置对话框。



【图8-17】证书设置对话框

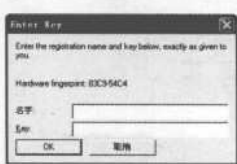


(7) 回到Armadillo主界面，选择保护菜单的“保护文件”选项，几分钟后会弹出软件保护成功对话框，如图8-18所示。单击“关闭”按钮，可以保存文件方便以后进一步分析。



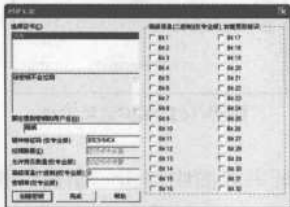
【图8-18】软件保护成功对话框

(8) 在电脑文件中双击“跳棋.exe”，弹出“Enter Key”对话框，要求输入名字和注册码，软件增加注册认证成功，如图8-19所示。



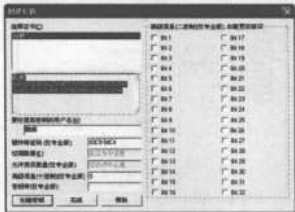
【图8-19】Enter Key对话框

(9) 注册软件可以通过Armadillo获取注册码。在Armadillo主界面，单击密钥菜单的“创建密钥”选项弹出“创建密钥”对话框，在选择证书中选中“跳棋”，在要注册到密钥的用户名中输入软件需要注册的用户名，这里输入“跳棋”，在硬件特征码（仅专业版）中输入“Enter Key”对话框中输入“Hardware fingerprint”后面的硬件码，单击“创建密钥”按钮，如图8-20所示。



【图8-20】创建密钥对话框

(10) 在创建密钥对话框中，显示用户名和注册码，如图8-21所示。



【图8-21】显示用户名和注册码

8.2.4 codefantasy软件加密解决方案

CodeFantasy软件加密解决方案是专门针对软件加密而设计，提供的加密算法包括对称算法、Hash算法、公开密钥算法、文件加密、文件Hash值、软件反跟踪、反静态分析、日期限制、次数限制、系列号、文件完整性校验、文件压缩和解密、简单Hash、其他算法。用户可以把这些算法直接导入软件，增强软件的安全性。

Codefantasy的加密解决方案安装非常简单，首先是安装好delphi的开发环境。

(1) 单击打开“Delphi”→“Component”→“Install Packages”命令，打开“Default Project Options”对话框。

(2) 单击“Add”按钮，在弹出的对话框中选择CodeFantasyPack.bpl所在的路径，然后单击“OK”按钮即可成功安装。

下面我们认识一下这些算法，在编程中可以借鉴。

1. 对称算法

AES128算法加密接口

功能：加密字符串

接口定义：function TACGuard. Fantasy3 (FantasyStr3a,FantasyStr3b:String) :String;

参数定义：FantasyStr3a为需要加密的字符串；FantasyStr3b为加密Key。

返回值类型：函数返回值类型为String型

2. Hash算法

MD5算法加密接口

功能：字符串加密。

接口定义：function TACGuard. Fantasy95 (FantasyStr95a) :String;

参数定义：FantasyStr95a为需要加密的字符串。

返回值类型：函数返回类型为String型。

3. 公开密钥算法

RSA-128位算法加密接口

功能：字符串加密。

接口定义：function TACGuard. Fantasy143 (FantasyStr143a,FantasyStr143b,FantasyStr143c:string) :String;

参数定义：FantasyStr143a为需要加密的字符串；FantasyStr143b为公钥模数；FantasyStr143c为公钥。

返回值类型：函数返回类型为String型。

4. 文件加密

AES128算法文件加密接口

功能：加密任意类型文件。

接口定义：function TACGuard. Fantasy49 (FantasyStr49a,FantasyStr49b,FantasyStr49c:String) :Boolean;

参数定义：FantasyStr49a为需要加密的文件；FantasyStr49b为加密后输出的文件；FantasyStr49c为加密Key。

返回值类型：返回值为Boolean型，TRUE为文件加密成功，FALSE为文件加密失败。

5. 文件Hash值

文件MD5 HASH值接口

功能：获取任意类型文件的MD5 HASH值。

接口定义：function TACGuard. Fantasy116 (FantasyStr116a) :String;

参数定义：FantasyStr116a为需要获取Hash值的文件名。

返回值类型：函数返回类型为String型。

6. 软件反跟踪

Anti-Loader for Win2000/XP

功能：进行反跟踪，如检测OllyDbg等工具。

接口定义：function TACGuard. Fantasy138 () :Boolean;

参数定义：无参数。

返回值类型：返回值类型为Boolean型，返回True表示软件被调试，返回False表示软件没被调试。

7. 日期限制

功能：天数限制接口

接口定义：function TACGuard. Fantasy154 (FantasyInt154a:integer) :Integer;

参数定义：FantasyInt154a为软件可以使用天数。

返回值类型：函数返回类型为String型。

8. 次数限制

次数限制接口

功能：设置软件可使用次数。

接口定义：function TACGuard. Fantasy153 (FantasyInt153a:integer;var OutputInt:Integer) : Boolean;

参数定义：FantasyInt153a为软件可以使用次数。

返回值类型：函数返回类型为String型。

9. 系列号

获取机器码接口

功能：获取IDE、SCSI硬盘、BIOS、CPU、MAC等的系列号并合并成一个系列号输出

接口定义：function TACGuard. Fantasy142 (var OutputStr:String) :Boolean;

参数定义：无参数。

返回值类型：返回值类型为String型。

10. 文件完整性校验

文件Crc32接口

功能：获取任意类型文件的CRC32校验值。

接口定义：function TACGuard. Fantasy135 (FantasyStr135a:string) :String;

参数定义：FantasyStr135a为需要获取校验值的文件完整路径。

返回值类型：函数返回类型为String型。

11. 文件压缩和解密

文件压缩加密接口

功能：在对文件压缩以后再对文件加密。

接口定义：function TACGuard. Fantasy155 (FantasyStr155a,FantasyStr155b,FantasyStr155c:String;CipherInt:TFantasyCipher) :Boolean;

参数定义：FantasyStr155a为要压缩加密的文件名；FantasyStr155b为压缩加密输出的文件名；FantasyStr155c为加密Key；CipherInt为加密要采用的算法。这个参数的值是固定的，用户只能输入“KBase64、KAes128、KAes192、KAes256、KRc2、KRc4、KRc5、KRc6、KDes、K3Des、KTea、KIdea、KRijndael、KSerpent、KMars、KMisty1、KBlowfish、KTwofish、KIce、KThinice、KIce2、KCast128、KCast256、KNone”中任意一个值，并且要注意区分大小写，KNone这个值的意思是只压缩不加密。

返回值类型：函数返回类型为Boolean型。

12. 简单Hash

简单Hash函数AP接口

功能：获取字符串的Hash值。

接口定义：function TACGuard. GetAPHash (InputStr:String) :String;

参数定义：Inputstr为需要获取Hash值的字符串。

返回值类型：函数返回类型为String型，该值就是字符串的Hash值。

8.3 共享软件解密

共享软件,通常都是“先使用后付费”的方式销售。根据共享软件作者的授权,用户可以从各种渠道免费得到它的拷贝,也可以自由传播它。用户总是可以先使用或试用共享软件,认为满意后再向作者付费;如果你认为它不值得你花钱买,可以停止使用。对于共享软件的加密技术,也是开发者常常讨论的问题。本着学习交流的精神,本节介绍一些常见的共享软件解密工具,主要是反汇编工具和脱壳技术,在阅读本节时,读者应该对汇编指令有一定的了解。

8.3.1反汇编解密

1.反汇编原理

通常编写程序都是利用高级语言如C等语言进行编程的，后再经过编译程序生成可以被计算机系统直接执行的执行文件。反汇编即是指将这些执行文件反编译还原成汇编语言或其他高级语言。但通常反编译出来的程序与原程序会存在许多不同，虽然执行效果相同，但程序代码会发生很大的变化，一般人很难读懂。

2. W32Dasm反汇编

W32Dasm是一个静态反汇编工具，也是破解人常用的工具之一，它也被比作破解人的屠龙刀。通常利用它来对欲破解的软件进行静态分析，静态分析即从反汇编出来的程序清单上分析。从提示信息入手进行分析，一般软件在设计时，采用人机对话方式。所谓人机对话，即在软件运行过程中，需要由用户选择的地方，软件即显示相应的提示信息，并等待用户按键选择。而在执行完某一段程序之后，便显示一串提示信息，以反映该段程序运行后的状态，是正常运行，还是出现错误，或者提示用户进行下一步工作的帮助信息。了解软件的编程思路，有利于破解。

【案例8-4】利用W32Dasm进行反汇编解密。

以W32Dasm无极版为例，运行程序，主界面如图8-22所示。



【图8-22】 W32Dasm主界面

下面我们就以ZTZ-IE网络浏览器1.7为例，所需软件：ZTZ-IE网络浏览器，W32Dasm及Ultraedit软件，具体步骤如下。

(1) 在W32Dasm的主界面，选择“反汇编”菜单，打开要汇编的程序，这里我们选择“ZTZ-IE网络浏览器1.7”程序。在没有破解前，运行ZTZ-IE网络浏览器，试着输入一下注册码，如图8-23所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 8 章 共享软件的加解密工具



【图8-23】ZTZ-IE网络浏览器注册界面

(2) 在W32Dasm的主界面，单击工具栏上的“Strn Ref”按钮，弹出“W32Dasm字符串参考列表”窗口，在“搜索”框，输入“密码”字样，单击“搜索”，出现很多结果，选择“密码正确，注册成功！”，双击该行。如图8-24所示。



【图8-24】W32Dasm字符串参考列表

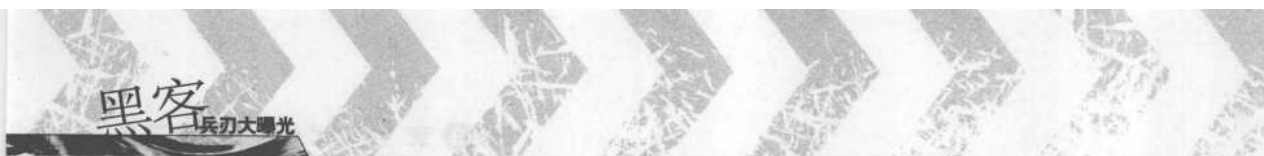
(3) 关闭字符串查询窗口，回到主界面，可以看到有“密码正确，注册成功”字样，如图8-25所示。



【图8-25】反汇编界面

(4) 代码分析：往上走，可以发现，有如下代码：
0046B64A 7533 jne 0046B67F---->这里就是要改的地方，不相等则跳到，程序之所以没有来到注册成功的地方主要就是因为这个跳转
:0046B64C BA0B000000 mov edx, 0000000B

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



```
* Possible StringData Ref from Code Obj ->"Yire"
```

```
:0046B651 B824B74600      mov eax, 0046B724
```

:0046B656 E839250000 call 0046DB94

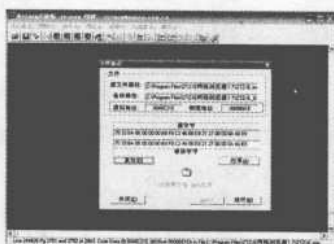
```
:0046B65B 6A40          push 00000040
```

* Possible StringData Ref from Code Obj ->"祝贺你"

```
:0046B65D B92CB74600      mov ecx, 0046B72C
```

* Possible StringData Ref from Code Obj ->"密码正确, 注册成功!"

在“0046B64A 7533 jne 0046B67F”处,右击选择“编辑”,查看它的实际地址,如图8-26所示。



【图8-26】文件修改

(5) 打开Ultraedit, 选择打开ztz-ic程序, 按快捷键“ctrl+G”, 输入0x6B61E, 其中0x表示十六进制把7533改为9090, 即输入的注册码不正确时来到对的地方, 正确时跳到出错的地方。

(6) 重新运行ZTZ-IE网络浏览器,输入任意注册码,均能成功,破解完成。

「案例8-5」利用C32asm进行反汇编解密。

C32asm是由国内的解密高手pll621编写的一款功能强大的反汇编工具，不仅拥有很快的反汇编速度，而且还有以下这些和反汇编相关的辅助功能：

- (1) 能同时对多个文件进行反汇编操作;
- (2) 能对文件进行16进制编辑, 而且支持直接编辑汇编语言代码, 再也不用去记源代码的机器码了;
- (3) 支持Unicode字符编码方式的字符串的读取, 比如W32Dasm不能正常反汇编出VB程序的中文字符串, 而C32asm可以做到;
- (4) 进程编辑, 比如可以对进程进行内存编辑, Dump正在运行的进程, 终止当前运行的进程等。

运行C32asm, 操作界面如图8-27所示。



【图8-27】 C32asm操作界面

C32asm共有两种工作模式：

(1) ASM模式

这是软件最基本的功能，提供快速的PE格式反汇编。此外还能提供输入表、输出表、参考字符、跳转、调用、PE文件分析等显示和导出；提供反汇编语句彩色语法功能，方便阅读分析，能方便自定义语法色彩；提供对ord调用和非ord调用的import自定义解析功能；提供方便的跳转、调用目标地址的代码显示；提供代码查找，快速定位；提供书签定位，代码注释，代码复制等多项实用功能。

(2) Hex模式

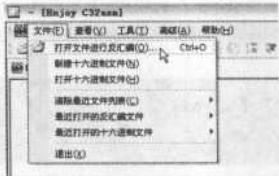
Hex模式是一个十六进制的文件编辑器，功能强大，可比HexWorkShop和WinHex，除去一些没有必要的功能外，可以算是一个专业的十六进制编辑工具。速度快，操作方便，功能齐全，是修改文件的一个强大工具。

可以16、10、8、2等多种进制方式显示Hex文件，有时这样的显示很方便。

多种方式选定数据块，多种自定义方式拷贝数据，多种方式粘贴数据，多种方式改变数据，多种数据格式查找数据，填充、插入数据，快速定位的书签功能，凡是方便的数据操作方式都具备。

使用C32asm，进行反汇编解密步骤如下：

(1) 单击执行“文件”→“打开文件进行反汇编”命令，打开待解密的可执行文件，如图8-28所示。这里打开一个lbgj.exe文件。



【图8-28】打开文件进行反汇编

(2) 查找关键提示字符“软件进入学习版状态，xxxx”，在反汇编软件中搜索“软件进入学习版状态”，找到并双击地址，定位到0x0040DDD0，如图8-29所示。



【图8-29】查找关键字并定位

(3) 分析代码，如图8-30所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图8-30】代码分析

其中，
::0040DDC4:: 8886 4C010000 MOV [ESI+14C],AL表示将值写入此地址，
::0040DDCA:: 75 0E JNZ SHORT 0040DDDA表示如果AL不是0，就跳转，我们
需要跳转。

（4）修改代码：
需要修改的是
::0040DDBF:: 0F95C0 SETNE AL，将AL值直接赋值非0。
首先，单击鼠标右键选择“0040DDBF”这行，选择“对应Hex编辑”，快速定位到EXE
文件，如图8-31所示。



【图8-31】定位到EXE文件

然后，直接选择“编辑”→“按地址切换”命令，切换到可修改的汇编模式，如图8-32所示。



【图8-32】可修改的汇编模式

接着，单击空格修改，
::0040DDBF:: 0F95C0 SETNE AL
改为：
::0040DDBF::B0 01 Mov AL, 1
NOP
如图8-33所示。最后，保存并自动生成Bak备份文件，文件破解完成。



【图8-33】修改代码

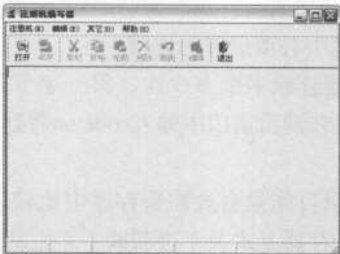
8.3.2制作内存注册机

目前有许多程序的注册码算法都与硬件有关，这类程序在每一台机上安装时都会生成一

个机器码，要把这个机器码E-MAIL给作者，待他收到机器码后，再算出注册码寄回给用户，一机一码的结果就是软件只能一机一用。本来这样无可厚非，但是有些时候，这样做给用户造成了不少的麻烦，因为只要用户重装系统或升级更换硬件，就要重新去注册软件。

【案例8-6】利用Keymake制作内存注册机。

Keymake是一款可以很方便地制作“注册机”或软件补丁的软件。之所以给“注册机”加上了引号，是因为严格说来，用Keymake来制作的“注册机”并不是真正的注册机，只能算做是软件的补丁或另类注册机，用Keymake制作的“注册机”在运行后，可以让注册码自己跳出来，直接显示在屏幕上。运行Keymake，打开操作界面，如图8-34所示。



【图8-34】Keymake界面

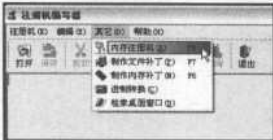
Keymake工具附带了一个KEY.EXE程序，如图8-35所示。



【图8-35】KEY.EXE程序

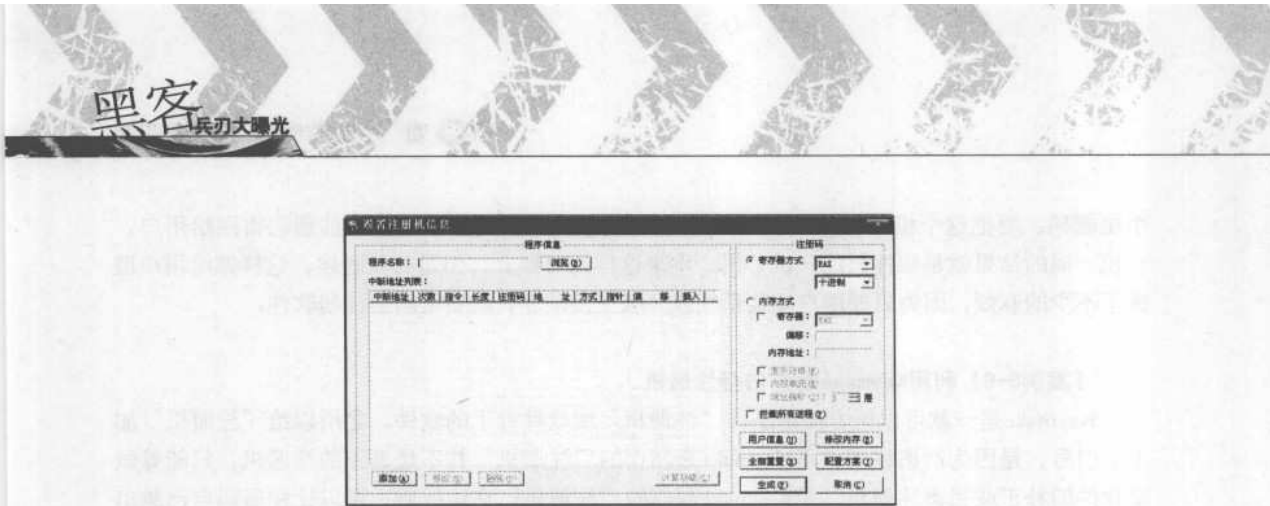
下面以为KEY.EXE制作内存注册机为例，其具体步骤如下：

- (1) 单击执行“其他”→“内存注册机”，或直接按F8，如图8-36所示。



【图8-36】执行“内存注册机”程序

- (2) 打开“设置注册机信息”对话框，如图8-37所示。在图中，可以设置注册机的诸多信息。



【图8-37】“设置注册机信息”对话框

“设置注册机信息”对话框中各项设置的说明：

- ①中断次数，即指在该位置连续中断多少次。第一字节，就是将当前设置的中断位置处反汇编后的第一个字节（可通过在调试窗口中输入code on看到）。指令长度就是当前中断位置反汇编后的长度。
 - ②寄存器方式，因为注册码可能是会放在寄存器中比较，并且可能经过十进制或十六进制的转换，所以就提供了一个寄存器方式及十进制或十六进制的选项。
 - ③内存方式，如设置为EDX，即指注册码保存在EDX所指向的内存地址中（而不是寄存器里）。
 - ④偏移地址，比如注册码是在eax+64的位置，那么现在就可以在偏移地址处填入64，如果是eax-64，就填入-64。
 - ⑤宽字符串，一般在VB程序中出现，用00将ASCII码分隔开。
 - ⑥内存单元，比如说注册码在[EAX]处看到1a,2b,3c,4d，并且它就是注册码，就可以使用这个选项。
 - ⑦地址指针，如果eax+64处的值是123456，而123456里的值又是654321，654321所指向的地址才是注册码所在地址，所以加入了一个“地址指针”，现在可以根据自己的需要设置了。比如说你要从654321里取注册码，就不要选择地址指针；如果你要从123456里取注册码就选择地址指针，并将值设置为1；如果你要从eax+64里取注册码就选择地址指针，将值设置为2。有了这个功能以后就可以尽量避免使用直接内存地址。因为Win2000/XP对内存的分配与Win98不同，直接指定内存地址很容易出错。
 - ⑧经过加壳，现在许多程序都用aspack、upx等工具进行了压缩，这个功能就是针对这类程序。
 - ⑨修改内存，主要是对于一些需要经过修改内存中的数据后，才会出现注册窗口或才能正常注册的程序。
 - ⑩如果生成的注册机出现错误，你可以在制作前单击全部重置，将所有数据置零。配置方案，让你可以对每一次的设置进行保存。在左边窗口处也设置保存注册码信息，是因为程序可能对注册码分次进行比较。
- (3) 首先单击“浏览”按钮，在随后的对话框中选择KEY.EXE，如图8-38所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图8-38】 打开KEY.EXE

(4) 然后单击“添加”按钮，打开“添加数据”对话框，如图8-39所示。

在这里需要进行一些设置。对于KEY.EXE，中断地址为4011F2，中断次数即指在该位置连续中断多少次，这里设置为1。第一字节，就是将当前设置的中断位置处反汇编后的第一个字节（可通过在调试窗口中输入code on看到），这里设置为FF。指令长度就是当前中断位置反汇编后的长度，这里设置为3。

单击“添加”按钮就把刚刚填完的内容加入到“设置注册机信息”对话框的“中断地址列表:”中。单击“关闭”按钮,关闭“添加数据”对话框,返回到“设置注册机信息”中。现在在“设置注册机信息”中选择“内存方式”,并且在“寄存器:”前面打上钩,在它的下拉列表框中选定EAX,偏移填上A,同时勾上“宽字符串”和“地址指针”,如图8-40所示。



【图8-39】“添加数据”对话框



【图8-40】 设置其他信息

(5) 单击“用户信息”按钮，打开“设置信息”对话框，如图8-41所示。

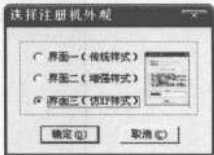
在这里可以为内存注册机设置一些信息，如软件的窗口标题，主页和邮件地址以及关于该软件的说明等。在“窗口标题”中输入任意内容，这里输入的是“KEY内存注册机”，在“你的主页”和“你的邮件”中输入你的相关信息即可，如果没有可以不填，这些内容会在你制作的内存注册机中显示出来。在“说明信息”中输入该文件的相关说明，这些说明的内容会在内存注册机运行界面中出现。可以输入该软件的使用方法和注意事项等，这里输入的“这是一个测试的KEY内存注册机”。

设置完毕后，单击“确定”按钮返回到“设置注册机信息”对话框中。

(6) 单击“生成”按钮,打开“选择注册机外观”对话框,让你选择生成的注册机的外观界面,如图8-42所示。



【图8-41】“设置信息”对话框



【图8-42】“选择注册机外观”对话框

有“界面一（传统样式）”和“界面二（增强样式）”以及“界面三（仿XP样式）”可供选择，我们选择“界面三（仿XP样式）”，然后单击“确定”按钮，选择好文件保存路径，并将该文件命名为“KEY内存注册机”，然后单击“保存”按钮就可以了，如图8-43所示。



【图8-43】“另存为”对话框

最后生成的文件是EXE格式，大小只有19KB。如果选择“界面一（传统样式）”则生成的文件体积更小。

(7) 内存注册机生成以后，运行“KEY内存注册机.exe”，如图8-44所示。

提示输入注册码，随便输入一个数字，例如12，单击“确定”按钮，KEY内存注册机将会运行，并生成一个注册码，如图8-45所示。



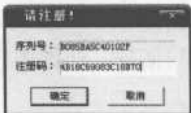
【图8-44】运行KEY内存注册机.exe



【图8-45】KEY内存注册机生成注册码

(8) 复制该注册码，并单击运行KEY.EXE，在“请注册”对话框中粘贴刚才由内存注册机生成的注册码，如图8-46所示。

单击“确定”按钮，打开“注册成功”对话框，如图8-47所示。



【图8-46】“请注册”对话框



【图8-47】“注册成功”对话框

8.4 暴力破解共享软件

“天下没有免费的午餐”，这个道理大家都懂。计算机发展到今天，各种各样的软件让人应接不暇，当然它也提供了很大的方便。虽然大部分的软件都可以在网上免费下载，但是下载后安装，你会发现这些软件都需要进行注册，就算可以用，也只是用几天左右就不行了，如果继续应用，必须要花费不少的“银两”。有没有办法可以避过注册这关呢？答案是肯定的，“道高一尺，魔高一丈”嘛。既然软件是人开发的，当然也有人可以破解了。而“爆破”也名“暴力破解”就是最常用的破解方法。

8.4.1 破解的原理及方法

破解的三个阶段：

初级：修改程序，用ultraedit等工具修改exe文件，称暴力破解，简称爆破

中级：追出软件的注册码

高级：写出注册机

先说这爆破。所谓爆破，就是指通过修改可执行文件的源文件，来达到相应的目的。举个例子，比如说某共享软件，它比较用户输入的注册码，如果用户输入的，跟它通过用户名（或其它）算出来的注册码相等（即用户输入的注册码正确了），那么它就会跳到注册成功的地方去，否则就跳到出错的地方去。

只要找到这个跳转指令，把它修改为需要的“造型”，就可以为所欲为了。

1. 在某软件中，这样来进行注册：

00451239 CALL 00405E02 (关键CALL，用来判断用户输入的注册码是否正确)

0045123D JZ 004572E6 (JZ--此为关键跳转，如果用户输入的注册码正确，就跳向成功处，即004572E6处)

0045XXXX YYYYYYYYYY

XXXXXXXXXX YYYYYYYYYY

XXXXXXXXXX YYYYYYYYYY

XXXXXXXXXX 执行到此处，会提示用户注册失败

...提示用户注册码不正确等相关信息

...

004572E6 ... <-- (注册成功处!!!)

...提示用户注册成功等相关信息

在软件执行到00451239处的时候，CALL置0045E02处来进行注册码判断。接着回来后就来了一个跳转语句，即如果用户输入的注册码正确就跳到004572E6处，就算是注册成功了。如果用户输入的注册码不正确的话，那么就不会在0045123D处进行跳转，而一直执行下去。在下面等它的，是注册失败部分。

只要把那个关键跳转JZ给改为JNZ（如果用户输入的注册码错误，就注册成功，输入正确

则注册失败）。当然你也可以将JNZ修改为Jmp，这样的话，你输入的注册码无论正确与否。都可以注册成功。

2. 我们再来讲一下另外一种情况：

00451239 CALL 00405E02 (关键CALL，用来判断用户输入的注册码是否正确)

0045123D JNZ 004572E6 (!!!<--此为关键跳转，如果用户输入的注册码不正确，就跳向失败处，即004572E6处)

0045XXXX YYYYYYYYYY

XXXXXXXXXX YYYYYYYYYY

XXXXXXXXXX YYYYYYYYYY

XXXXXXXXXX 执行到此处，就提示用户注册成功

...提示用户注册成功等相关信息

...

004572E6 ... <--(注册失败处!!!)

...提示用户注册码不正确等相关信息

与前一种情况不同的，就是第一种情况：如果注册码正确，就跳到注册成功处，如果没有跳走，就会执行到失败处。而这一种情况则是如果注册码不正确，就跳到注册失败处，否则将执行到注册成功处。

这种情况的修改，除了把JNZ改为JZ外，还可以改为Nop，Nop这个指令没有任何意义，将该条指令修改为Nop后，便可随意输入注册码注册。

原理知道了，下面我们再来讲一下具体的修改办法。

首先需要了解虚拟地址和偏移量转换。在SoftICE和W32Dasm下显示的地址值是所谓的内存地址（memory offset），或称之为虚拟地址（Virtual Address，VA）。而十六进制工具里，如：Hiew、Hex Workshop等显示的地址就是文件地址，称之为偏移量（File offset）或物理地址（RAW offset）。

所以当需要通过那些十六进制工具来对可执行文件中的相应指令进行修改，先要找到它的File offset。没有必要去使用那些专门的转换工具，在W32Dasm中就有这个功能，比如W32Dasm中来到0045123D处，在W32Dasm界面下方的状态栏中就会出现该条指令的虚拟地址和偏移地址，即@:0045123D @offset 0005063Dh 后面的这个0005063Dh就是相应的偏移地址。得到该地址后，便可用UltraEdit等十六进制工具来对可执行文件进行修改了。比如使用UltraEdit，先用UltraEdit打开可执行文件，然后按“Ctrl+G”，接着输入你得到的偏移地址，就可以来到相应的机器码处。

所谓的机器码，就是看到的那些个十六进制数据，它们与汇编指令是一一对应的。

以下这几个是爆破时要用到的：

JZ=74;JNZ=75;JMP=EB;Nop=90

爆破的时候，只要对以上机器码进行相应的修改就行了，比如第一种情况，可以将74修改为EB，即将JZ修改为JMP。而第二种情况，则需将75修改为90，即将JNZ修改为Nop。

在前面讲爆破的时候提到的CALL，一般情况下，就是对两个注册码（一个是软件自身通

过用户的注册名或机器什么的计算出来的正确的注册码，令一个就是你输入的错误的注册码）进行比较。在CALL之前一般会把所用到的数据先放到一个地方，CALL过去的时候再从这些地方把先前放入的数据取出来，进行相应的处理。这个关键CALL也是这样，在CALL之前，一般会把那两个注册码放到堆栈或某个寄存器中。只要在调试器中，单步执行到该CALL，在未进去之前通过CALL之前的指令判断正确的和不正确的注册码放到哪里了，然后再用相应指令查看就可以了。

下面列出两个最常见的情况（可参考相关教程）：

mov eax [] 这里可以是地址，也可以是其它寄存器

mov edx [] 同上，该条指令也可以是pop edx

call 00?????? 关键call

test eax eax

jz (jnz) 或jne (je) 关键跳转

在关键CALL之前，软件会把两个注册码分别放入eax和edx中，你只要在CALL处下d eax或d edx就能看到正确的注册码了。

mov eax [] 这里可以是地址，也可以是其它寄存器

mov edx [] 同上，该条指令也可以是pop edx

call 00?????? 关键call

jne(je) 关键跳转

8.4.2 爆破的条件

要进行爆破，除了自身的计算机知识的丰富外，一定的工具必不可少，这正如战场上的士兵一样，必须有武器，要不只能束手待毙。

1. 爆破工具

(1) 必须要熟悉一款十六进制编辑器，推荐用HEX Workshop，可以到天空软件站进行软件下载。

Hex Workshop 是一款非常专业的十六进制编辑器，功能强大的开发工具，可以方便地进行十六进制编辑、插入、填充、删除、剪切、复制和粘贴工作，配合查找、替换、比较以及计算校验和等命令使工作更加快捷。速度快，算法精确，并附带计算器和转换器工具。如图8-47所示的操作界面。



【图8-48】Hex Workshop操作界面

(2) WIN32DASM反汇编器

Win32dasm是个反编译工具，它可以将应用程序静态反编译为win 32汇编代码，利用Win32dasm可以对程序进行静态分析，帮助快速找到程序的破解突破口，有时甚至可以直接用它来破解软件，如图8-48所示的操作界面。有这两样就可以，初学者万不要贪多求全。精通一两件，其它触类旁通、举一反三。



【图8-49】Win32dasm是个反编译工具

2. 会使用以上工具

不会使用爆破工具，就仿佛一个上战场的士兵没有了枪。怎样去爆破呢？靠猜？如果对设置密码的人不熟悉，就没有办法猜测。猜测法依靠的是经验和对目标用户的熟悉程度。现实生活中，很多人的密码就是姓名汉语拼音的缩写和生日的简单组合。甚至还有人用最危险的密码——与用户名相同的密码。这时候，猜测法拥有最高的效率。但是如果不熟悉呢？咱们还是循规蹈矩吧。

3. 必须会汇编

如果现在不会，可以先找一些经典的教程，对照上面的程序和方法做下实验。如果成功了，自然，你的信心就加强了，也有兴趣了。那么就赶快开始学汇编吧。

4. 最重要的是有信心、耐心以及恒心

8.4.3 快速找爆破点

要进行爆破，最重要的对爆破点的正确选择。也就是说必须要在众多的死胡同里面找到出路，路找对了，当然是一片光明；路错了，只会越陷越深。爆破点的选择一般可以遵守下面的原则。

1. 用Win32DASM反汇编并保存工程文件

注意：IDA PRO功能很强大，但是它体积也非常庞大，没有完美汉化版，最令人受不了的是速度非常的慢！不推荐初学者使用。

2. 在反汇编文件中找到可疑点

在反汇编文件中找到突破点，比如“恭喜”、“注册成功”、“注册码错误”、“无效的注册码”、“Thank you”、“Sorry”等。但是事实上，只有极少数的软件只修改注册判断就可以，所以要把更多的注意力转移到其他的可疑点上去，比如“未注册标识”、“过期警告”、“次数标识”、“NAG对话框”等，找到后，一般向上不远处就可以看到条件转移语句JZ、JNZ、JLE等。所以，熟练使用各种工具的搜索功能也是基本功之一。如图8-49所示的在Win32DASM反汇编的软件中找到的“Thank you”的字样。



【图8-50】找到“Thank you”的字样

3. 如果找不到，可以利用EXESCOPE中的对话框或字符串的ID号和地址指针，通过一定的转换，可在反汇编文件中找到相应的提示。

一般的有这样的参数入栈：
PUSH 00000064（64即为ID号为100）

注意：Win32DASM里的提示不是完全对，它解释很清楚，“Possible”，“可能是”。

4. 在十六进制编辑软件中搜索到提示信息的起始地址，把它换成程序运行时的偏移地址。如你得到地址是004DE356，那么回到Win32DASM中搜索6856E34D00，（它就是：PUSH 004DE356）如果能找到一处或两处就表示找对了。有很多程序蛮狡猾的，不一定行得通。

注意：关于爆破教程中程序代码地址问题：爆破教程中都会放上一部分程序代码以帮助讲解程序的分析方法，例如下面的一段程序代码：

```
.....
0167:00408033  PUSH  00
0167:00408035  PUSH  EBX
0167:00408036  CALL  [USER32!EndDialog]
0167:0040803C  JMP   0040812C
.....
```

在这里程序中的代码地址如0167:00408033，其代码段的值（即0167）有可能会有区别，不一定一模一样，但偏移值应该是固定的（即00408033不变），所以如果看到爆破文章里的程序代码的地址值和自己的电脑里不一样，不要以为搞错地方了，只要你的程序代码正确就不会有问题。

5. 找到注册判断函数CALL（子程序）

通常软件的程序内部都会利用一个子程序（即 CALL *****）去验证输入的注册码正确与否，对于注册码显式存在的程序，一般都会将所输入的注册码和正确的注册码放进寄存器，然后调用验证子程序进行判断，将结果返回，应用程序根据子程序返回的结果决定是否注册成功，这样的程序经常具有如下的形式（具体的可以参考上图3）：

```
****:***** MOV EAX,[*****]      (或 PUSH EAX等形式)
****:***** MOV EDX,[*****]      (或 PUSH EDX等形式)
****:***** CALL *****
****:***** TEST EAX,EAX           (或 TEST AL,AL, 或是没有这一句等形式)
****:***** JNZ *****           (或 JZ *****等形式)
```

其中EAX和EDX指向的内存区域就是输入的注册码和正确的注册码，这里的寄存器EAX和EDX是随意写的，也可以是ECX，EBX，EDI，ESI等等。对于注册码隐式存在的程序，虽然不能直接看到正确的注册码，但是通常也是先将所输入的注册码地址放进某个寄存器，然后调用子程序去验证，爆破时就需要进入子程序去分析注册算法。总之，看到子程序（call *****）后面跟着跳转指令（JNZ *****或JZ *****）的地方就应该提高警惕，多用DEAX（或EBX、ECX、EDX、EDI、ESI...等）去看看寄存器指向的内存区域藏着什么东西。



看见程序中使用下面这个函数要注意，即GetDlgItemInt，这个API函数的作用是将输入的文本转化为整数，所以这类程序中是不会有显示存在的注册码的，因为注册码被转换为整数了，程序通常会用 CMP ECX, EDX 这种类型的指令去验证注册码的正确性，这里ECX和EDX中存的就是所输入注册码和正确注册码的整数形式，此时可以用 ? edx 和 ? ecx 看到它的十进制形式，即我们输入的形式。

注意：如果你找到的CALL在程序中被调用了二三十次，那肯定不是了，顶多是字符串比较函数罢了。只一次的程序少，一般是在三到六次之间。

6. 通过以上可疑点，最好能找准注册标志变量，一种是固定内存变量，在程序中事先就定义好的。一般有以下几种比较形式：

```
mov eax, dword ptr [00401078]
cmp eax, 00000001
jz ...
```

```
mov eax, dword ptr [00401078]
test eax, eax
jz ...
```

```
mov eax, dword ptr [00401078]
mov ebx, dword ptr [eax]
cmp ebx, 00000000
jnz ...
还有一种是利用堆栈偏移的临时变量，如：
mov eax, dword ptr [ebp+50]
cmp eax, 00000001
jz ...
```

还有几种与前面的几种类似，这里由于篇幅的原因，就不一一举例了。

7. 最好能分析一下程序的结构和流程。

到这里找准爆破点应该没问题了。

8.4.4 进行爆破

当找准爆破点后，你会发现有很多种爆破的方法都可以达爆破的目的。

1. 修改转移语句

一般的更改方法是，首先把程序分为不需要跳和需要跳的两类：

(1) 不需要跳，就把74XX, 75xx, 0F84xxxxxxxx, 0F85xxxxxxxx…中的xx, xxxxxxxx（偏移量）改为00, 00000000。

(2) 需要跳，就把74, 75改为EB，把0F84, 0F85改为90E9。这可避免万一有正确的注册码反而会出错的事情发生。

2. 修改注册标志变量

如变量为1则为注册，为0则为未注册，那么你只要搜索所有将该变量置0的语句改为置1就行了。

```
mov eax, 00000000
mov dword ptr [00401078], eax
这种好改。但大多是这样：
xor eax, eax
mov dword ptr [00401078], eax
```

这种有些难度，它不是简单地送值，而是异或置0。xor eax, eax的机器码是33C0，只有两个字节，而mov eax, 00000001的机器码是B801000000有五个字节。可以这样改：把CC30改为B001。为什么要这样改呢？因为B001就是mov al, 01。一般情况下这样改都不会有问题。

3. 修改判断函数CALL

如果这个函数只是判断注册是否正确，并返回AX的值，一般会这样改。在CALL入口处就改为B801000000C3，就是：

```
mov eax, 00000001  
ret
```

这样可少执行代码，并且不访问注册表。甚至可把后面死码都置为00。

4. 修改次数限制

如果某些软件，你进行爆破后，没有出现注册提示，但用起来还是有次数的限制。这时候就需要修改次数限制，使程序一直认为低于这个限制值就行了。

【案例8-7】破解的软件为FTP搜索器。

下面做一个爆破实例，破解的软件为FTP搜索器（Scanftp v1.0）

（1）首先判断软件是否加了壳，如果加了壳，就要先脱壳。FTP搜索器是没有加壳的，有个简单的方法判断，在注册页面随便输入一串字符后，注册错误它进行了提示。比如，我输入的注册码为http://www.forbidden404.com，提示注册错误，如图8-51所示。



【图8-51】注册失败错误提示

（2）然后运行Ollydbg（OD）程序，打开scanftp.exe，查找错误提示，如图8-52所示。



【图8-52】用OD载入需要破解的软件程序

（3）找到CALL语句，下面的MOV DH AL上单击鼠标右键，在弹出的菜单上选择“Ultra字符串参考”→“查找ASC II”命令，如图8-53所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第⑧章 共享软件的加解密工具



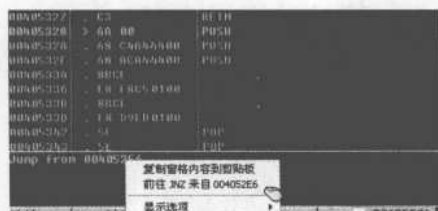
【图8-53】 查找ASCII字符

(4) 找到字符串“请检查注册码是否正确”，如图8-54所示，然后双击之。



【图8-54】找到字符串“请检查注册码是否正确”

(5) 这时就可以找到入口地址,如图8-54的第一行所示。在下面的Jump from 004052E6上单击鼠标右键,在弹出的菜单中选择“前往INZ来自004052E6”。



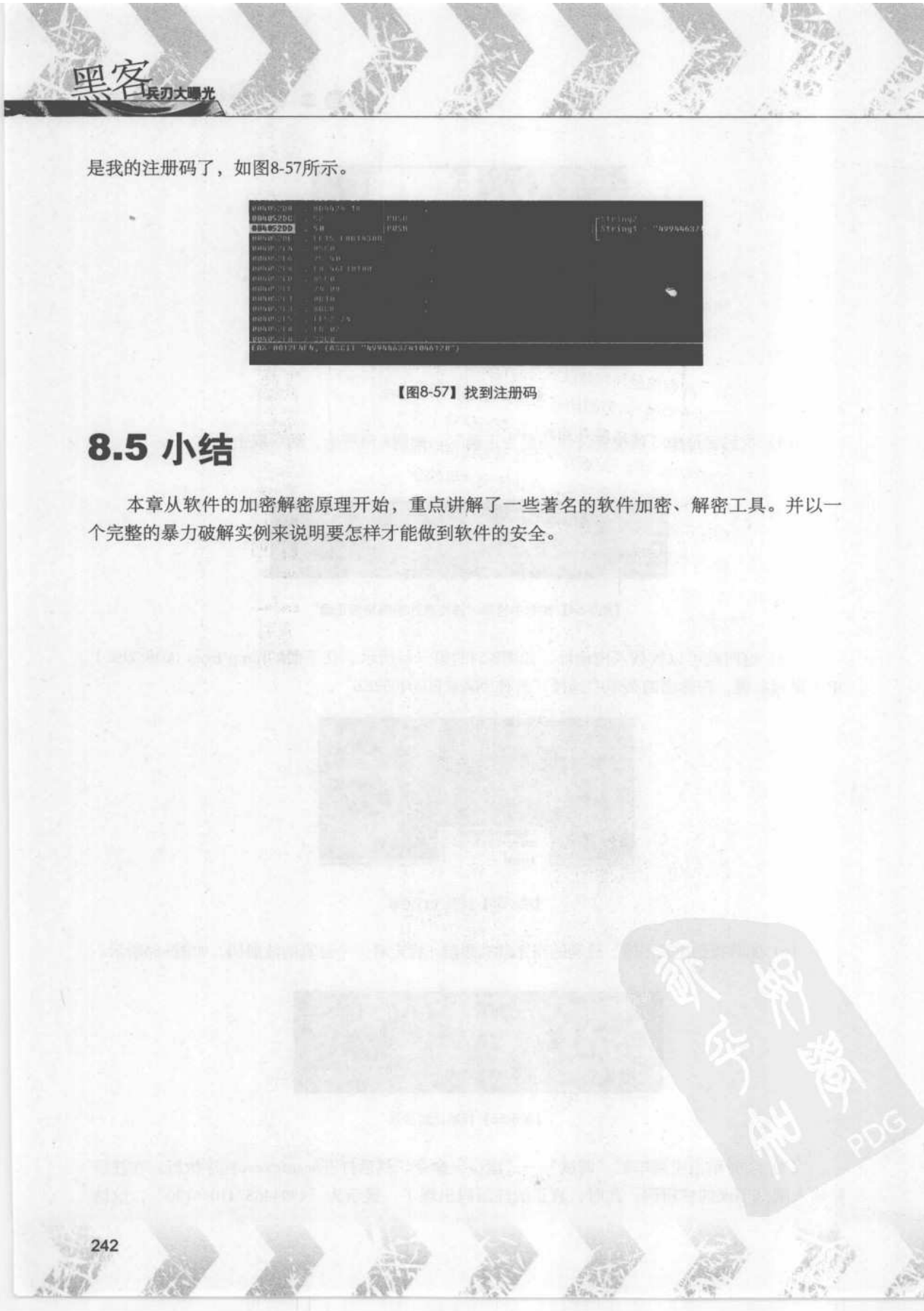
【图8-55】找到入口地址

(6) 此时找到比较函数，胜利的曙光就在眼前。肯定有一个是真的注册码，如图8-56所示。



【图8-56】找到比较函数

(7) 此时单击主菜单栏“调试”→“运行”命令。然后打开Scanftp.exe程序执行。在注册栏输入刚才错误的注册码。此时，真正的注册码出现了，显示为“4994463741046120”，这就



【图8-57】找到注册码

8.5 小结

本章从软件的加密解密原理开始，重点讲解了一些著名的软件加密、解密工具。并以一个完整的暴力破解实例来说明要怎样才能做到软件的安全。

第9章 远程控制工具

远程控制，即在网络上由一台电脑（主控端Remote/客户端）远距离去控制另一台电脑（被控端Host/服务器端）的技术。谈到远程控制，不可避免地要提到木马，因为木马是一种最常见的基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。木马是一种客户端/服务器模式的应用程序，黑客使用安装了木马客户程序（控制方软件）的机器为客户机，而感染了木马服务器程序的机器为待攻击的目标机。在介绍完木马的基础知识后，本章将通过实例介绍几种远程控制工具的使用。

本章要点

- ◎ 了解木马的基本概念
功能及其工作方式
- ◎ 了解不用种木马的追踪
防范方法
- ◎ 掌握常用的远程控制工
具的使用

9.1 木马介绍

“木马”全称是“特洛伊木马（Trojan Horse）”，原指古希腊士兵藏在木马内进入敌方城市从而占领敌方城市的故事。在Internet上，把这种利用程序从内部打开端口的以便黑客攻击的方式，起名为特洛伊木马。可从网络上下载的应用程序或游戏外挂、或网页中，包含了可以控制用户的计算机系统或通过邮件盗取用户信息的恶意程序——木马，它可能造成用户的系统被破坏、信息丢失甚至系统瘫痪等。

木马究竟是如何工作的？它究竟能实现哪些功能？如何防止木马程序潜入系统呢？

本节将介绍几种常见类型的木马，并通过实际操作演示其追踪防范方法。

9.1.1 木马的功能和分类

木马除了具有基本的远程控制功能外，还包含极大的破坏性。不同的木马通常又具有各自的特殊功能。

1. 木马的主要功能：

(1) 窃取密码

一切以明文的形式、“*”形式或缓存在CACHE中的密码都能被木马侦测到。此外，很多木马还提供击键记录功能，它将会记录服务端每次敲击键盘的动作，所以一旦有木马入侵，密码将很容易被窃取。

(2) 文件操作

控制端可通过远程控制对服务端上的文件进行删除，新建，修改，上传，下载，运行，更改属性等一系列操作，基本涵盖了Windows平台上所有的文件操作功能。

(3) 修改注册表

控制端可任意修改服务端注册表，包括删除，新建或修改主键、子键和键值。有了这项功能，控制端就可以禁止服务端光驱的使用，锁住服务端的注册表，将服务端上木马的触发条件设置得更隐蔽。

(4) 系统操作

这项内容包括重启或关闭服务端操作系统，断开服务端网络连接，控制服务端的鼠标，键盘，监视服务端桌面操作，查看服务端进程等，控制端甚至可以随时给服务端发送信息。

2. 木马的分类

自木马程序诞生至今，已经出现了多种类型，想一次就完全地列举和说明是不太可能的。尽管如此，给木马程序作一个分类，对计算机使用者来说，也是非常必要的。

根据木马程序的作用来分，木马可以分为以下九种类型。

(1) 远程控制类木马：这类木马数量最多，危害最大，同时知名度也最高。它可以让攻击者完全控制被感染的计算机，攻击者可以利用它完成一些甚至连计算机主人本身都不能顺利进行的操作。

(2) 密码发送木马：专门为了盗取被感染计算机上的密码而编写的。木马一旦被执行，就会自动搜索内存，Cache，临时文件夹以及各种敏感密码文件，一旦搜索到有用的密码，木马就会利用免费的电子邮件服务将密码发送到指定的邮箱，从而达到获取密码的目的，这类木马大多使用25号端口发送E-mail。

(3) 键盘记录密码：这种特洛伊木马是非常简单的。它们只做一件事情，就是记录受害者的键盘敲击并且在LOG文件里查找密码。它们有在线和离线记录这样的选项，分别记录用户在线和离线状态下敲击键盘时的按键情况。也就是说用户按过什么按键，下木马的人都知道，从这些按键中很容易就会得到用户的密码等有用信息。

(4) 破坏性质的木马：这种木马惟一的功能就是破坏被感染计算机的文件系统，使其遭受系统崩溃或者重要数据丢失的巨大损失。从这一点上来说，它和病毒很相像。不过，一般来说，这种木马的激活是由攻击者控制的，并且传播能力也比病毒逊色很多。

(5) Dos攻击木马：这种木马的危害不是体现在被感染计算机上，而是体现在攻击者使用上。使用者可以利用它来攻击一台又一台计算机，给网络造成很大的伤害和损失。

(6) 代理木马：黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的。通过代理木马，攻击者可以在匿名的情况下使用Telnet,ICQ,IRC等程序，从而隐蔽自己的踪迹。

(7) FTP木马：这种木马可能是最简单和古老的木马了，它的惟一功能就是打开21端口，等待用户连接。现在新FTP木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而进入对方计算机。

(8) 程序杀手木马：这类木马的功能就是关闭对方机器上运行防木马程序，如ZoneAlarm, Norton Anti-Virus等，让其他的木马更好地发挥作用。

(9) 反弹端口型木马：由于防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。因此这类木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定时监测控制端的存在，发现控制端上线立即弹出端口主动连结控制端打开的被动端口。为了隐蔽起见，控制端的被动端口一般开在80，这样，即使用户使用端口扫描软件检查自己的端口，稍一疏忽就可能会以为是自己在浏览网页。

根据木马的特点及其危害范围，木马又可以分为以下五大类。

(1) 网游木马：由于网络游戏产业超高速发展，网上虚拟装备交易非常火爆。一些别有用心病毒者把目光盯在这一安全性比较薄弱的环节，用户如果中了针对网络游戏的木马，用户账号会被盗取，并立即转移账号中的游戏装备，再由木马使用者卖出这些盗取的游戏装备而获利。

(2) 网银木马：网银木马专门针对网络银行攻击，采用记录键盘和系统动作的方法盗取网银的账号和密码，并发送到作者指定的邮件，直接导致用户的经济损失。

(3) 即时通讯木马：可以利用即时通讯工具（比如：QQ、MSN）进行传播。中了这类木马后电脑会下载病毒作者指定的任意程序，危害不可谓不大。

(4) 后门木马：该木马在网络中被恶意者大量传播。它本身不具有传播的功能，都是被恶意者种植。该木马病毒采用反弹端口技术绕过防火墙，对被感染的系统进行远程文件和注册

表的操作,可以捕获被控制的电脑的屏幕,可远程重启和关闭计算机,可以禁用系统热键和注册表编辑器,中了该木马后,被感染的系统将完全暴露于黑客手中。

(5) 广告木马病毒: 此类木马采用各种技术隐藏于系统内, 修改IE等网页浏览器的主页, 禁用多种系统功能, 收集系统信息发送给传播广告木马的网站。甚至修改网页定向, 导致一些正常的网站不能登录。

9.1.2 木马的隐藏方式

由于木马所从事的是“地下工作”, 因此它必须隐藏起来, 想尽一切办法不让用户发现它; 它不是自己生成一个启动程序, 而是依附在其他程序之中。有些木马把服务器端和正常程序绑定成一个程序的软件, 用户使用绑定的程序时, 木马也入侵了系统。甚至有个别木马程序能把它自身的.exe文件和服务端的图片文件绑定, 在用户浏览图片的时候, 木马便侵入了该用户的系统。

木马实现隐藏主要通过以下六种方式:

1.在任务栏里隐藏

这是最基本的隐藏方式。如果用户看到任务栏中出现一个来历不明的图标, 肯定会起疑心。因此, 木马虽然在用户启动系统时会自动运行, 但它不会在“任务栏”中产生图标。

2.在任务管理器里隐藏

如果在打开任务管理器的时候, 可以看见一个木马程序在运行, 那么这肯定不是什么好木马。所以, 木马会千方百计地伪装自己, 尽量不出现在任务管理器里。通常, 木马通过把自己设为“系统服务”欺骗操作系统。

3.端口隐藏

一台机器有65536个端口, 其中1024以下的端口是常用端口, 用于一些常用的服务。如Web服务常用的80端口, FTP服务常用21端口等。大多数木马使用的端口在1024以上, 而且呈越来越大的趋势; 当然也有占用1024以下端口的木马, 但占用这些端口可能会造成系统不正常, 这样的话, 木马就会很容易暴露。也许用户知道一些木马占用的端口, 或许会经常扫描这些端口, 但现在的木马都提供端口修改功能, 这么多端口用户很难全部注意到。

4.隐藏通讯

隐藏通讯也是木马经常采用的手段之一。任何木马运行后都要和攻击者进行通讯连接。或者通过即时连接: 如攻击者通过客户端直接接入被植入木马的主机; 或者通过间接通讯: 如通过电子邮件的方式, 把侵入主机的敏感信息送给攻击者。现在大部分木马一般在占领主机后会在1024以上不易发现的高端口上驻留; 有一些木马会选择一些常用的端口, 如80、23, 有一种非常先进的木马还可以做到在占领80HTTP端口后, 收到正常的HTTP请求仍然把它交与Web服务器处理, 只有收到一些特殊约定的数据包后, 才调用木马程序。


5.隐藏加载方式

木马加载的方式可以说千奇百怪, 无奇不有。但殊途同归, 都为了达到一个共同的目的, 那就是诱使用户运行木马的服务端程序。如果木马不做任何伪装, 就告诉用户这是木马,

2. 通过Win.ini文件启动

Windows利用扩展名为.ini的文件保存Windows及其应用程序的初始化信息，每次启动时，都会从相应的INI文件中读取初始化设置信息，并据此进行配置。

Win.ini文件包含若干个域，每一个域由一组相关的设定组成。其中一个主要的域是[Windows]，它影响Windows的操作环境部分，包括在启动Windows时执行哪一个应用程序，警告声音的设置、窗口边框的宽度、键盘响应的速度、鼠标器设置以及将文件定义为文档或程序等。[Windows]域中的“load=”和“run=”两个项目会在Windows启动时运行，与启动组相同，这两个项也会出现在msconfig中，如图9-2所示。



```
run=c:\windows\file.exe
load=c:\windows\file.exe
```

【图9-2】 Win.ini文件启动

3. 通过注册表启动

(1) 通过注册表项：

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run],

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]和

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]。

这是很多Windows程序都采用的方法，也是木马最常用的。使用非常方便，但也容易被发现，由于应用太广，所以几乎提到木马，就会让人想到这几个注册表中的主键。通常木马会使用最后一个键值。

使用Windows自带的程序：msconfig，或注册表编辑器（在“开始”→“运行”中执行“regedit”命令）都可以将注册表中的启动项轻易地删除，所以这种方法并不十分可靠。但可以在木马程序中加一个时间控件，以便实时监视注册表中自身的启动键值是否存在，一旦发现被删除，则立即重新写入，以保证下次Windows启动时自己能被运行。这样木马程序和注册表中的启动键值之间形成了一种互相保护的状态。木马程序未中止，启动键值就无法删除（手工删除后，木马程序又自动添加上了）；相反的，不删除启动键值，下次启动Windows还会启动木马。

(2) 通过注册表项：

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce],

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]和

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]。

这几个键值下的项目和上一种相似，会在Windows启动时启动，但Windows启动后，该键值下的项目会被清空，而且它的内容不会出现在msconfig中，因而不易被发现。这种方法的隐蔽性比上一种方法好，但是只能启动一次。这三个键值中通常木马会选择第一个，因为在第二个键值下的项目会在Windows启动完成前运行，并等待程序结束才会继续启动Windows。

在这种情况下木马如何发挥效果呢？其实很简单，虽然只能启动一次，但木马启动成功后可以再在这里添加一次，下次系统启动时木马又会随之启动。当然，如果在启动的时候添加，虽说添加的项目不会出现在msconfig中，但在regedit中却可以直接将其删除。

还有一种方法，不在启动的时候而是在退出Windows的时候添加注册表项，这要求木马程序本身有截获Windows消息的功能。当发现关闭Windows消息时，暂停关闭过程，添加注册表项目，然后才开始关闭Windows，这样用regedit也找不到它的踪迹了。不过，这种方法也有个缺点，就是一旦Windows异常中止，木马也就失效了。

4. 通过system.ini文件启动

在system.ini文件的[boot]域中的“shell=”项的值在正常情况下是“explorer.exe”，这是Windows的外壳程序，换一个程序就可以彻底改变Windows的面貌。可以在“explorer.exe”后加上木马程序的路径，这样Windows启动后木马也就随之启动，而且即使是安全模式启动也不会跳过这一项，这样木马也就可以保证永远随Windows启动了，这时，如果木马程序也具有自动检测添加shell项的功能的话，那简直是天衣无缝的绝配。

但这种方式也有个先天的不足，因为只有shell这一项，如果有两个木马都使用这种方式实现自启动，那么后来的木马可能会使前一个无法启动，可以算是以毒攻毒。

5. 通过某个特定文件或程序启动

(1) 寄生于特定程序当中

这种方式即将木马和正常程序绑定，有点类似于病毒，程序在运行时，木马程序先获得控制权或另开一个线程以监视用户操作，从而截取密码等。这类木马编写的难度较大，需要了解文件结构和相关的Windows的底层知识。

(2) 将特定的程序改名

这种方式常见于针对QQ的木马，例如将QQ的启动文件QQ200x.exe，改为QQ200x.ico.exe（Windows默认是不显示扩展名的，因此它会被显示为QQ2000b.ico，而用户会认为它是一个图标），再将木马程序改为QQ200x.exe，此后，用户运行QQ，实际是运行了QQ木马，再由QQ木马去启动真正的QQ，这种方式实现起来也要比上一种简单的多。

(3) 文件关联

通常木马程序会将自己和TXT文件或EXE文件关联，这样当用户打开一个文本文件或运行一个程序时，木马也就神不知鬼不觉地启动了。

这类通过特定程序或文件启动的木马，发现比较困难，但查杀这类木马并不难。一般地，只要删除相应的文件和对应的注册表键值即可。

6. 通过“组策略”启动

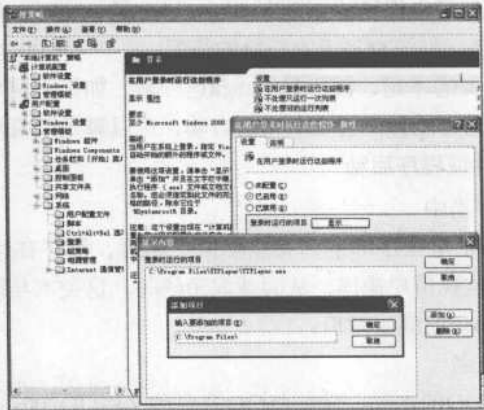
这种启动方式鲜为人知，单击“开始”→“运行”命令，在弹出的“运行”对话框中执行“gpedit.msc”命令，打开“组策略”对话框，如图9-3所示。可以看到，“本地计算机策略”中有两个选项：“计算机配置”与“用户配置”。展开“用户配置”→“管理模板”→“系统”→“登录”，双击“在用户登录时运行这些程序”子项进行属性设置，选定“设置”项中的“已启用”项并单击“显示”按钮弹出“显示内容”窗口，再单击“添加”按钮，在“添加项目”窗口内的文本框中输入要自启动的程序的路径，单击“确定”按钮就完成了。

重新启动计算机，系统在登录时就会自动启动你添加的程序，如果刚才添加的是木马程序，那么一个“隐形”木马就这样诞生了。因为用这种方式添加的自启动程序在系统的“系统配置实用程序”是找不到的，同样在我们所熟知的注册表项中也找不到，所以非常危险。

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]和
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]中，而是在注册表的：

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]项内。

如果怀疑自己的电脑被种了“木马”，可是又找不到它在哪儿，建议到注册表的[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]项里找找，或是进入“组策略”的“在用户登录时运行这些程序”看看有没有启动的程序。



【图9-3】通过“组策略”启动木马



在“组策略”中添加的自启动程序，虽然也会出现在注册表中，但不在我们熟悉的注册表项。

9.2 木马追踪防范

一旦你的机器变为养马场，你就没有任何的秘密。木马的主人可以随时查看他想要的信息，所以一定要对木马有所防范。

9.2.1 DLL木马追踪防范

要了解DLL木马，首先要知道什么是“DLL”。

“DLL”是动态链接库（Dynamic Link Library）的简称，动态链接技术是把通用的函数写入一些独立的文件里面，作为库文件，即DLL文件。在编译时，并不把库文件加进程序，而是把它做成已经编译好的程序文件，给它们开个交换数据的接口。程序员写程序的时候，一旦要用到某个库文件的一个功能函数，系统就把这个库文件调入内存，连接上这个程序占有的任务进程，然后执行程序要用的功能函数，并把结果返回给程序显示出来；完成需要的功能后，这个DLL文件停止运行，整个调用过程结束。在我们看来，就像是程序自己带有的功能一样。

DLL文件可以被多个程序调用，只要在代码里加入对相关DLL的调用声明就能使用它的全部功能，但是，它不能独立运行。操作系统在加载DLL的时候，需要一个入口函数，否则系统无法引用DLL。调用DLL文件中的函数有两种方式：

加载时动态连接：调用方模块显示地调用以导出DLL函数。为DLL创建导入库，然后将DLL链接到应用程序。在加载应用程序时，导入库提供加载DLL和查找导出的DLL函数所需的信息。

运行时动态链接：在运行中加载DLL时，调用方模块使用LoadLibrary 函数或LoadLibraryEx 函数。调用方模块调用GetProcAddress函数以获取导出的DLL函数的地址。由于DLL文件在运行时必须由程序文件调用，Windows就为DLL技术做了标准规范。让一个DLL文件设置几个接口，每个接口都标明它的功能，程序只要根据标准规范找到相关接口就可以调用DLL了。这个接口就是“应用程序接口”（Application Programming Interface），每个DLL带的接口都不相同，尽最大可能的减少了代码的重复。

1. 动态嵌入式 DLL木马介绍

（1）动态嵌入技术

Windows中，每个进程都有自己的私有内存空间，别的进程是不允许对这个私人领地进行操作的，但是，实际上仍然可以利用种种方法进入操作进程的私有内存，这就是动态嵌入，它是将自己的代码嵌入正在运行的进程中的技术。动态嵌入有很多种，最常见的是钩子、API以及远程线程技术，现在的大多数DLL木马都采用远程线程技术把自己挂在一个正常系统进程中。

远程线程技术就是通过在另一个进程中创建远程线程（Remote Thread）的方法进入那个进程的内存地址空间。在DLL木马的范畴里，这个技术也叫做“注入”，当载体在那个被注入的进程里创建了远程线程并命令它加载DLL时，木马就挂上去执行了，没有新进程产生，要想让木马停止惟有让挂接这个DLL木马的进程退出运行。但是，很多时候我们只能束手无策——它和explorer.exe挂在一起了，你确定要关闭Windows吗？

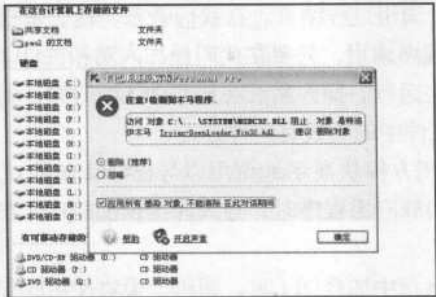
（2）DLL与木马

DLL是编译好的代码，虽然它不能独立运行，需要程序调用，但是它与程序很相似，仅仅是接口和启动模式不同，只要改动一下代码入口，DLL就可以变成一个独立的程序。因此，可以把DLL文件看作是缺少了main入口的EXE程序，DLL的各个功能函数可以看作一个程序的几个函数模块。DLL木马就是把实现了木马功能的代码，加上一些特殊代码写成DLL文件，导出相关的API，在别人看来，这只是一个普通的DLL，但是这个DLL却携带了完整的木马功能，这就是DLL木马的概念。

在系统启动的时候，一个EXE程序会将DLL加载至某些系统进程（如explorer.exe）中运



行，这样一来，普通的进程管理器就很难发现这种木马了。而且即使发现了也很难清除，用户无法在资源管理器中删除这个DLL文件，因为只要木马寄生的进程不终止运行，那么这个DLL就不会在内存中被卸载。由于DLL运行时是直接挂在调用它的程序的进程中的，并不会产生新的进程，所以它的隐蔽性很好，相对于传统的EXE木马，他很难被发现，如图9-4所示DLL木马程序。



【图9-4】DLL木马程序

(3) DLL木马的执行入口

DLL木马的标准执行入口为DllMain，所以必须在DllMain里写好DLL木马运行的代码，或者指向DLL木马的执行模块。DLL木马模块与API库是不一样的，DLL木马可以导出几个辅助函数，但是必须有一个过程来负责主要执行代码，否则这个DLL就是一堆零碎的API函数了。如果涉及一些通用代码，可以在DLL里写一些内部函数，供自己的代码使用，而不是把所有代码都开放成接口。

(4) DLL木马的启动

由于DLL不能独立运行，需要一个EXE文件使用动态嵌入技术挂上其他正常的进程，让被嵌入的进程调用这个DLL的DllMain函数，激发木马运行。最后，启动木马的EXE程序结束运行，DLL木马启动完毕。

启动DLL的EXE是个重要角色，它被称为Loader。Loader可以是多种多样的。Windows的rundll32.exe经常被一些DLL木马用来做了Loader，这种木马一般不带动态嵌入技术，它直接挂着rundll32进程运行，用rundll32的方法像调用API一样去引用这个DLL的启动函数激发木马模块开始执行，即使你杀了rundll32，木马本体仍然存在。

注册表的AppInit_DLLs键也被一些木马用来启动自己，如求职信病毒。利用注册表启动，就是让系统执行DllMain来达到启动木马的目的。因为它是kernel调入的，对这个DLL的稳定性有很大要求，稍有错误就会导致系统崩溃，所以很少看到这种木马。

有一些更复杂点的DLL木马通过svchost.exe、smss.exe、winlogon.exe等关键系统进程启动，这种DLL木马必须写成NT-Service，入口函数是ServiceMain，一般很少见，但是这种木马的隐蔽性也不错，而且Loader有保障。

2. DLL木马的清除

通过以上对DLL木马原理的介绍，可以看出这类木马的隐蔽性很强，一旦感染很难清除。

具体防范措施如下：

- 经常查看启动项（注册表、服务等），看看有没有多处莫名其妙的项目，这些启动项目往往是DLL木马的Loader所在。
- 经常用杀毒软件进行查杀，或安装网络防火墙。
- 定时备份硬盘上的文件，不要运行来路不明的软件和打开来路不明的邮件。

虽然中了DLL木马很难清除，但并不是说完全没有办法。前面讲过，DLL木马不能独立运行，它必须通过其他程序调用才能“作恶”，因此，要清除DLL木马，就要先找到调用它的进程，针对不同的调用进程采取不同的方法来清除。

通过rundll32.exe启动木马是最简单的方法，rundll32.exe是系统自带的动态链接库工具，可以用来在命令行下执行动态链接库中的某个函数。如果发现系统中有rundll32.exe这个进程在运行，那很有可能就是木马。不过系统有时也会调用rundll32.exe来加载正常的DLL文件，这时就要通过注册表项查看加载的是什么DLL文件。

『案例9-1』清除通过rundll32.exe启动的DLL木马。

(1) 终止rundll32.exe进程：同时按下“Ctrl + Alt + Del”组合键打开“Windows任务管理器”，单击“进程”选项卡，如图9-5所示。选中rundll32.exe进程，然后单击“结束进程”按钮；或右键单击该进程，在弹出的快捷菜单上单击“结束进程”命令。



【图9-5】终止rundll32.exe进程

- (2) 单击“开始”→“运行”命令，在“运行”对话框中输入regedit命令，找常用的注册表启动键值，删除跟在rundll32.exe之后的陌生的DLL文件，并记下该DLL文件路径和文件名。
- (3) 根据记下的路径，在系统中找到该DLL文件删除即可。

『案例9-2』清除注入普通进程的DLL木马。

对于利用iexplorer.exe和explorer.exe这两个进程启动的DLL木马，其清除也是比较方便的。如果DLL文件是注入到iexplorer.exe进程中，由于此进程就是IE浏览器进程，因此需要先关掉所有IE窗口和相关程序，然后直接找到DLL文件执行删除就可以了。

如果DLL文件是注入到explorer.exe进程中，那么就略显麻烦一些。由于此进程用于显示桌



面和资源管理器，因此，当通过任务管理器结束掉explorer.exe进程后，桌面无法看到，桌面上所有图标消失掉，同时，也无法打开资源管理器找到木马文件进行删除。怎么办呢？

实际上，解决的方法也很简单。在任务管理器中单击菜单“文件”→“新任务运行”，打开“创建新任务”对话框，单击“浏览”按钮，通过浏览对话框就可以打开DLL文件所在的路径，如图9-6所示。然后选择“文件类型”为“所有文件”，即可显示并删除DLL文件了。



【图9-6】在浏览对话框中删除DLL文件

许多木马注入到svchost.exe、smss.exe、winlogon.exe等系统关键进程中，这些进程使用普通方式无法结束，使用特殊工具结束掉进程后，却又很可能造成系统崩溃无法正常运行。

例如一款著名的木马PCShare采用了注入winlogon.exe进程的方式运行，由于winlogon.exe是掌握Windows登录的进程，手工无法卸载，使用某些查杀木马工具卸载时会出现异常重启，根本来不及清除掉DLL文件，重启后DLL文件又自动加载。对于这类DLL木马，必须在进程运行之前阻止DLL文件的加载，利用“System Safety Monitor”（简称SSM）可以实现这一功能。

SSM是一款俄罗斯出品的系统监控软件，通过监视系统特定的文件（如注册表等）及应用程序，达到保护系统安全的目的。这款软件功能非常强大，可以辅助防火墙和杀毒软件更好的保护系统安全。

【案例9-3】使用“System Safety Monitor”终结DLL木马。

(1) 运行System Safety Monitor程序，在程序界面中选择“规则”→“库文件”选项卡，如图9-7所示。



【图9-7】System Safety Monitor库文件规则设置界面

(2) 右键单击空白处，选择“编辑规则”→“添加文件规则”命令，弹出文件浏览对话框。在其中选择木马DLL文件，这里我们假设DLL木马文件名为test.dll，如图9-8所示：



【图9-8】选择要添加规则的库文件

(3) 单击“打开”按钮，该文件就被添加到“System Safety Monitor”的规则列表中，如图9-9所示，文件规则设置完成后单击“应用设定”按钮保存规则设置。



【图9-9】添加文件规则成功

(4) 更改System Safety Monitor启动设置。单击选择“选项”→“常规”命令，选中“自动启动”确保System Safety Monitor随系统启动而启动。设置成功后重启系统，这时SSM就会自动阻止相关进程调用“test.dll”木马文件。这样，该木马文件便不会被任何程序使用，在硬盘中找到该文件，直接删除即可。

9.2.2 网页木马追踪防范

网页木马是在用户浏览网页的时候悄悄地进入用户的计算机中的，很多用户浏览网页时被种入了木马，但自己却毫不知情。网页木马是怎样瞒过用户进入计算机中的呢？

1. 网页木马介绍

网页木马又被称为远程木马，它的核心是一个html网页。但是这个网页和其他网页有点不同，它是黑客精心制作的，木马文件捆绑在网页里，能够随网页自动打开。用户一旦单击了该网页就会感染木马。网页木马专门利用系统或软件的漏洞，通常是浏览器漏洞，当用户浏览网

页木马。

(5) 图片木马：其功能和Flash木马相似，以GIF、JPG等图片格式为结尾，打开的时候会显示图片，但同时也悄悄地打开了木马。

2. 网页木马防范

互联网的普及，使得网页木马日益猖獗，因此，在浏览网页的时候一定要有防范意识，做好防御工作。下面这些措施可以有效降低网页木马入侵的几率。

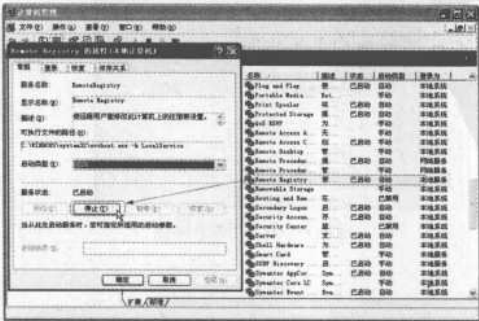
(1) 升级到IE6.0以上，安装最新的安全补丁，尽量使用FlashGet等多线程下载工具下载。

(2) 设定安全级别。在IE菜单栏中选择“工具”→“Internet选项”菜单项打开“Internet选项”对话框，选择“安全”选项卡，如图9-13所示，选中“Internet”后单击下面的“自定义级别”按钮，在弹出的“安全设置”对话框中，将安全级别设置为“高”。另外，可以将“ActiveX控件和插件”、“脚本”中的相关选项设置为“禁用”或者“提示”。需要注意的是，如果选择了“禁用”，一些需要使用正常ActiveX控件和脚本的网页可能无法正常显示。



【图9-13】Internet选项

(3) 禁止“远程注册表”服务。如果黑客通过木马连接到了计算机，而且计算机启用了远程注册表服务（Remote Registry），那么黑客就可远程设置注册表中的服务，因此远程注册表服务需要特别保护。关闭方法：单击“开始”→“控制面板”→“管理工具”→“服务”，用鼠标右键单击“Remote Registry”，然后在弹出的快捷菜单中选择“属性”命令，在“常规”选项卡中单击“停止”按钮，如图9-14所示。



【图9-14】禁止“远程注册表”服务

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



(4) 安装防毒杀毒和防木马软件。虽然杀毒软件并非万能，但这是最简单的防毒方法，只要及时地更新病毒库，计算机还是比较安全的，如图9-15所示Norton 杀毒软件2007。



【图9-15】Norton 杀毒软件2007

9.2.3 反弹式木马追踪防范

本章开篇讲到过，木马是一种客户端/服务器模式的应用程序。普通的木马是驻留在用户计算机里的一段服务器程序，而攻击者控制的则是相应的客户端程序。服务器程序通过特定的端口，打开用户计算机的连接资源；攻击者通过客户端程序发出请求与被植入木马的服务器段建立连接。

随着防火墙技术的发展，这种工作模式的木马很难起作用。因为攻击者必须与用户主机建立连接，木马才能工作，而在防火墙将严密地检查下，这样的木马连接请求常常被拒之门外。

1. 反弹式木马介绍

反弹式木马采用的是反向连接技术，它可以有效穿透防火墙。反弹式木马设计者在分析了防火墙的特性后发现：防火墙对于连入的请求往往会进行非常严格的过滤，但是对于连出的请求却疏于防范。

于是，反弹式木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口，木马程序定时监听控制端的存在，一旦发现控制端上线立即弹出端口主动连结控制端打开的被动端口。为了隐蔽起见，控制端一般使用80端口，这样，防火墙很可能会把这个连接当成是用户向外发起的HTTP请求。即使用户使用端口扫描软件检查自己的端口，发现的也是类似TCP连接，稍不注意就会以为是自己在浏览网页。如图9-16所示的“网络神偷”就是反弹式木马。



【图9-16】“网络神偷”

2. 反弹式木马防范

防范木马，良好的上网习惯还是关键：不要轻易运行陌生的程序，发现后缀为.EXE的文

件一定要特别小心，不要随便打开陌生人发来的邮件。

使用个人防火墙，如《天网个人防火墙》，也能阻止反弹式木马的入侵。《天网防火墙》采用“内墙”方式，专门对付存在于用户计算机内部的各种不法程序对网络的应用，可以有效地防御像“反弹式木马”这种的骗取系统合法认证的非法程序。当用户计算机内部的应用程序访问网络的时候，必须经过防火墙的内墙的审核。合法的应用程序被审核通过；而非法的应用程序将会被天网防火墙个人版的“内墙”拦截。

9.3 远程控制软件介绍

了解了木马的工作原理，看到木马如此隐蔽、功能如此强大之后，大家一定很想见识一下真正的木马吧。本节就给大家介绍几款经典的木马软件，详细讲解怎样来使用这些工具。

9.3.1 冰河

冰河是一款广泛流传的国产特洛伊木马，它凭借简单易用、功能强大的优势在网络吸引了无数的崇拜者，成为目前国内感染率最高的木马。

虽然自从2000年3月，冰河的原作者发布了冰河V2.2版本之后，就停止了开发，但网络上很多人开始了对冰河后续版本的发展，出现了如冰河V2.2改良版本、冰河V3.0[YZKZERO专版]、冰河V3.3[OICQBOY专版]等等，其功能都是大同小异。本文将以冰河V8.4[NEWFUN专版]为例演示这款经典木马的使用。

冰河既然是木马的一种，那么它的服务器和客户端两部分是不可或缺的。冰河的服务器端程序文件名通常为G_server.exe，运行于被控制端；客户端文件名通常为G_client.exe，黑客就是通过这个文件进行控制的。

有了服务器端和客户端程序后，首先要做的是想办法把服务器端程序植入到目的主机中，植入方法有很多，如通过捆绑、欺骗或是伪装为图片等方法，最终将服务器程序注入受控主机中并让它运行。

成功以后冰河木马会在对方计算机的Windows主目录下System32目录中生成kernel32.exe和Sysexplr.exe两个程序。接着冰河木马在没有任何提示的情况下自动运行kernel32.exe，并打开计算机的TCP端口7626，即将7626端口设置为监听状态。这时我们运行冰河木马的客户端，程序运行主界面如图9-17所示：



【图9-17】冰河木马客户端程序界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



服务器端植入成功后，客户端必须要先建立与服务器的连接才能进一步进行控制。通过在客户端添加主机就能轻松建立起这个连接。

【案例9-4】将被植入冰河木马的主机添加到冰河客户端。

- (1) 单击工具栏上的“添加主机”图标或选择“文件”→“添加主机”菜单，打开“添加计算机”对话框。
- (2) 配置主机信息，如图9-18所示。其中“显示名称”是自己定义的，显示在冰河“文件管理器”中的名称；主机地址为目标主机的IP地址；口令也是用户任意指定的，连接到目标主机时使用；监听端口默认是7626，用户也可以自己选择其他端口号。单击图9-10中的“确定”按钮，添加主机完成。
- (3) 添加完成后，冰河主界面上的文件管理器中就会显示新主机名称及其中的文件和文件夹，如图9-19所示。



【图9-18】添加主机



【图9-19】文件管理器

如果不知道哪台电脑中了冰河木马怎么办呢？不用担心，冰河客户端提供了搜索功能，可以自动搜索用户指定IP地址段内所有感染了冰河的电脑。

【案例9-5】搜索网络中感染了冰河的计算机。

- (1) 单击主界面上的“自动搜索”按钮，或选择“文件→自动搜索”菜单，打开的“搜索计算机”对话框。
- (2) 在“搜索计算机”对话框中输入待搜索的IP地址段、端口号和时延，单击“开始搜索”按钮即可自动进行搜索。搜索结果显示在右边的文本框中，如图9-20所示，显示格式为“状态:IP地址”。列表中状态为OK的IP地址，即表示感染了冰河木马的计算机。在该实例中搜索到IP地址为“192.168.0.100”和“192.168.0.24”两台主机。



【图9-20】搜索感染“冰河”的计算机

注意：搜索计算机每次只能对一个端口号进行搜索，如果植入冰河时选择其它端口号，自动搜索是检测不到的。

(3) 搜索结束后单击“关闭”按钮，返回到主界面，这时文件管理器中会自动会显示搜索结果中状态为OK的主机，如图9-21所示。



【图9-21】搜索计算机结果

找到目标计算机后，就可以利用冰河木马控制这台计算机了。冰河木马能够实现查看目标机器的屏幕，自动跟踪屏幕变化，记录各种口令信息，获取系统信息，限制系统功能，操作文件，修改注册表，发送信息等功能。下面通过案例看一下各个功能的具体实现。

【案例9-6】利用冰河木马查看目标机器屏幕。

(1) 单击工具栏上的“查看屏幕”按钮，或选择菜单项“文件→捕获屏幕”，弹出“图像参数设定”对话框，如图9-22所示。

(2) 设置图像格式，冰河支持JPEG和BMP两种图片格式。通过拖动游标选择图像的色深和品质，游标越靠右图像越清晰，但这时会降低传输速度。设置完成后单击“确定”按钮，这时就可以在新打开的“图像显示”窗口中看到对方屏幕了，如图9-23所示。



【图9-22】图像参数设定



【图9-23】冰河木马查看对方屏幕

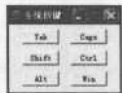
该窗口显示的是受控主机当前的屏幕截图，是一个静态的画面。如果想要对对方屏幕进行操作，就要用到冰河的控制屏幕的功能了。



【案例9-7】利用冰河木马控制对方屏幕。

(1) 打开“控制屏幕窗口”：单击主界面上的“控制屏幕”按钮，或单击“文件→屏幕控制”菜单，弹出和查看屏幕相同的“图像参数设定”对话框，按同样的方式设置图像属性即可。设置完成后弹出的“控制屏幕窗口”也和查看屏幕时相似，只是这时显示的是对方的实时状态，标题栏上会不断显示“正在接收数据……”的字样。

(2) 除了“控制屏幕窗口”外，系统还会弹出一个“系统按键”的小对话框，如图9-24所示。该对话框上的按钮对应相应的系统功能键。例如，按下“系统按键”对话框上的“Win”按钮，将打开目标主机的“开始”菜单，就像是在该主机本地按下键盘上的Windows窗口按键一样，如图9-25所示。



【图9-24】“系统按键”对话框



【图9-25】系统按键——“Win”按钮演示

(3) 在“屏幕控制窗口”中可以对目标主机进行各种各样的操作，和操作本地机器完全相同。但是控制端的这些操作将会全部显示在对方的屏幕上，这样，任何人都会发现自己的电脑正在被别人控制，攻击者就完全暴露了。所以，聪明的黑客通常不会直接在对方屏幕上进行操纵。不过，为大家能够对屏幕控制功能加深印象，我们再来看一个案例。

【案例9-8】利用冰河木马查看目标主机任务管理器。

有一定电脑基础的读者可能都知道，同时按下键盘上的Ctrl + Alt + Del快捷键可以打开任务管理器查看当前正在运行的程序和进程。可是，冰河的系统按键没有提供Del键，怎么办呢？

- (1) 打开“开始”菜单，方法前一个案例已经讲过。
- (2) 单击“运行”命令，在“运行”对话框中输入“taskmgr.exe”命令，如图9-26所示。



【图9-26】通过运行打开任务管理器

- (3) 单击“确定”按钮，“Windows任务管理器”就打开了。选择“进程”选项卡查看

一下目标主机上当前正在运行的进程，如图9-27所示。



【图9-27】查看目标主机进程

从图9-27里面的任务管理器中，可以看到“Kernel32.exe”这个进程，这就是我们的冰河木马服务器程序运行时挂接的进程。由于“Kernel32.exe”是一个系统进程，一般的用户看到这个进程可能会以为是系统正常的调用而忽略它，真正的冰河木马就被隐藏掉了。

“冰河信使”可以说是使冰河一举成名的最主要功能，它能以聊天室的形式同被控端进行在线交谈。

『案例9-9』使用“冰河信使”。

(1) 单击冰河客户端主界面上的“冰河信使”按钮，或菜单“文件”→“冰河信使”，打开“冰河信使”窗口，图9-28所示。在“冰河信使”窗口底部的文本框中输入要发送给被控端的信息，单击“发送”按钮即可。



【图9-28】冰河信使——客户端

(2) 消息发送后，对方屏幕上也会弹出“冰河信使”窗口，消息的内容显示在窗口上半部分的文本框内，如图9-29所示。



【图9-29】冰河信使——服务器端

在冰河主界面上还有另外一个大的功能模块——命令控制台，使用这些命令，能够完成本地机器上所能实现的所有功能，而且可以不在被控端屏幕上表现出来。

命令控制台主要的命令包括：

- (1) 口令类命令：系统信息及口令、历史口令、击键记录；
- (2) 系统类命令：捕获屏幕、发送信息、进程管理、窗口管理；
- (3) 控制类命令：鼠标控制、系统控制、其他控制；
- (4) 网络类命令：创建共享、删除共享、查看网络信息；
- (5) 文件类命令：文本浏览、查找、压缩、复制、删除、打开文件、目录增删、目录复制；
- (6) 注册表读写类命令：键值的读取、写入和重命名，浏览、增删、复制、重命名主键；
- (7) 设置类命令：更换墙纸、更改计算机名、更改服务器配置。

由于口令种类较多，我们仅以两个口令为代表讲述使用方法。

【案例9-10】利用冰河木马查看被控主机的系统信息。

- (1) 打开“命令控制台”，双击“口令类命令”或单击其左边的“+”将该节点展开。
- (2) 单击“系统信息及口令”子节点。
- (3) 单击右下部分的“系统信息”按钮，对方电脑的详细信息就将显示在文本框中，如图9-30所示，其中包括该主机的计算机名、用户名、内存大小、分区数及各分区的容量和剩余空间等信息。



【图9-30】利用冰河查看系统信息

【案例9-11】利用冰河操作目标主机注册表。

- (1) 浏览主键：展开“注册表读写”节点，单击“主键浏览”。
- (2) 在“主键”所对应的文本框中输入要查询主键的完整键名，如该例中查看“HKEY_LOCAL_MACHINE\SOFTWARE\”主键的键值及其子键，单击“浏览”按钮。浏览主键命令执行结果如图9-31所示：

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图9-31】利用冰河浏览目标机器注册表主键

(3) 写入键值：在“命令控制台”中单击“键值写入”命令，从浏览的结果中选择键名为“781”的子键作为示范。输入主键“HKEY_LOCAL_MACHINE\software\”；键名“781”；数据类型可以选择二进制、整数、字符串和字符串数组等类型，这里选择“字符串”；键名设为我们希望的键名，如“NewValue”，如图9-32所示。设置完成后单击“写入键值”按钮，新的键值就写入成功。



【图9-32】写入键值

(4) 读取键值：完成了写入键值之后我们再通过“读取键值”命令来查看一下新写入的键值，输入刚才新写入的主键和键名，单击“读取键值”按钮，结果如图9-33所示。



【图9-33】读取键值

冰河木马的功能非常强大，限于篇幅不能一一演示，有兴趣的读者可以亲自体验一下。从一定程度上可以说冰河是最有名的木马，就连刚接触电脑的用户也听说过它。虽然许多杀毒软件可以查杀它，但国内仍有几十万感染冰河的电脑存在。作为木马，冰河创造了最多人使用、最多人中弹的奇迹。

【案例9-12】清除冰河方法。

- (1) 删除C:\Windows\system下的Kernel32.exe和Sysexplr.exe文件。
- (2) 冰河会在注册表：HKEY_LOCAL_MACHINE/software/microsoft/Windows/CurrentVersion Run下扎根，键值为C:/Windows/system/Kernel32.exe，删除它。
- (3) 在注册表的HKEY_LOCAL_MACHINE/software/microsoft/Windows/CurrentVersion/Runservices下，还有键值为C:/Windows/system/Kernel32.exe的，也要删除。
- (4) 最后，改注册表HKEY_CLASSES_ROOT/txtfile/shell/open/command下的默认值，由中木马后的C:/Windows/system/Sysexplr.exe %1改为正常情况下的C:/Windows/notepad.exe %1，即可恢复TXT文件关联功能。

9.3.2 广外女生

广外女生是广东外语外贸大学“广外女生”网络小组的处女作，作为一个远程控制软件它可以运行于Win98、Windows2000/XP/2003或已经安装Winsock2.0的Win95/97上。

广外女生木马的基本功能很多。

- 文件管理：上传、下载、删除、文件重命名、文件属性设置、建立文件夹和运行指定文件等。
- 注册表操作：使用模拟的Windows注册表编辑器，随意编辑目标机器的注册表，让远程注册表编辑工作如同在本机上操作一样方便。
- 屏幕控制：随意控制对方屏幕，可以自定义图片的质量来减少传输的时间，可以全屏操作对方的鼠标（包括单击，双击，右键，拖动等鼠标事件）。
- 其他功能：远程任务管理、邮件通知、邮件服务等。

广外女生的一个特点是它的服务器木马程序可以使目标机器上的防火墙失去作用，这样连用户防火墙都不能察觉出木马程序的攻入。

广外女生客户端程序运行主界面如图9-34所示：



【图9-34】广外女生客户端程序主界面

为了防止用户误运行了服务器端程序而导致自己感染木马，广外女生的服务器端程序由客户端生成，首先来看一看生成服务器端程序的方法。

【案例9-13】生成广外女生服务器端程序。

(1) 单击主界面上的“服务端设置”选项卡，设置界面如图9-35所示。

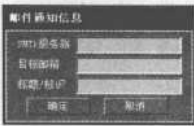


【图9-35】广外女生 - 服务端设置

(2) 在图9-35所示的界面中，可以选择“默认值”，应用默认的设置，也可以选择“自定义”对服务端程序做基本的设置。其中，“防火墙处理”一栏里，如果某一项被选中，则服务器端对应的防火墙或杀毒软件将失去作用。

(3) 设置完成以后单击“生成服务端”，广外女生的客户端软件就自动在客户端的同一目录下生成了默认名为GDUFS.exe的可执行木马服务端程序。

(4) 还可以在生成服务器端程序的时候，添加“邮件通知信息”的功能。在“服务端”设置界面中的“对方邮件通知列表”文本框中单击右键，选择“添加”命令，在弹出的“邮件通知信息”窗口中输入客户端用户的邮箱，图9-36所示，确定后再生成GDUFS.exe，这样只要目标机器上的用户运行GDUFS.exe，GDUFS.exe就会定期向指定邮箱发送电子邮件，通知控制端用户植入机器的IP地址和其他一些系统信息。



【图9-36】邮件通知信息

服务器端程序生成之后，接下来就该想办法把它植入到目标机器中，引诱目标机器用户运行。一旦GDUFS.exe运行，就会立即在TCP 6267端口进行监听，同时尝试关闭系统中的防火墙，这样立刻轻松掌握了目标机器的所有管理员权限。

找到了被感染的主机，广外女生客户端就能控制它了。客户端可以控制的范围包括：

- 密码记录：获取目标机器的管理员密码。
- 屏幕控制：控制目标机器的屏幕显示，或截取目标机器的当前屏幕。

- 进程管理：显示和中止目标机器中的进程。
- 远程注册表控制：显示和修改目标机器注册表信息。
- 文件共享：秘密打开目标计算机共享功能，暴露对方硬盘上的数据。
- 远程关机：直接关闭目标计算机。
- 向对方发送消息：向对方发送自定义消息。

使用这些控制功能很简单，只需要单击相应的标签进行一些设置即可，这里不再赘述。

【案例9-14】清除广外女生。

- (1) 由于该木马程序运行时无法删除该文件，因此启动到纯DOS模式下，找到System目录下的Diagcfg.exe，删除它；
- (2) 由于Diagcfg.exe文件已经被删除了，因此在Windows环境下任何EXE文件都将无法运行。找到Windows目录中的注册表编辑器“Regedit.exe”，将它改名为“Regedit.com”；
- (3) 回到Windows模式下，运行Windows目录下的Regedit.com程序(就是刚才改名的文件)；
- (4) 找到HKEY_CLASSES_ROOT\exefile\shell\open\command，默认键值改成"%1 %*";
- (5) 找到HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current-Version\RunServices，删除其中名称为“Diagnostic Configuration”的键值；
- (6) 关掉注册表编辑器，回到Windows目录，将“Regedit.com”改回“Regedit.exe”。

9.3.3 黑洞

黑洞是一个国产远程监控软件，主要用于个人管理和监控自己的电脑，或用于企业管理人员监控员工电脑。黑洞程序也可以被黑客利用成为木马工具，它的可怕之处在于强大的杀进程功能。也就是说控制端可以随意终止被控端的某个进程，如果这个进程是诺顿之类的防火墙，黑洞可以使得防火墙的保护功能全无，黑客由此长驱直入，在系统中肆意纵横。

我们使用的黑洞版本是2007V1.6版，运行黑洞2007客户端程序，首次运行将出现是“系统设置”窗口，包括“监听端口”、“连接密码”、“远程屏幕选项”和“超时设置”。

“监听端口”是指客户端等该服务端连接的TCP端口。注意监听端口不能使用系统已经使用的端口，否则会绑定失败，可单击“测试”按钮查看端口是否可用。如图9-37所示，我们选择8000端口，测试结果8000端口可以使用。

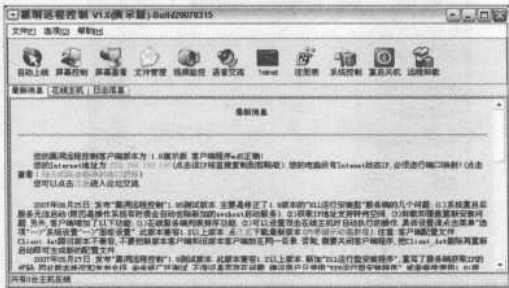


【图9-37】监听端口设置

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“连接密码”由用户自己指定；“远程屏幕选项”设置屏幕显示的颜色格式，有65536色、256色和16色，默认为256色；“超时限制”指定连接超时的毫秒数（0表示永远等待），当超过指定时间后服务端还没有反应，则自动取消此次传输，客户端用户应根据实际的网络传输速度进行设置。

设置完成后单击“确定”按钮，程序运行的主界面如图9-38所示：



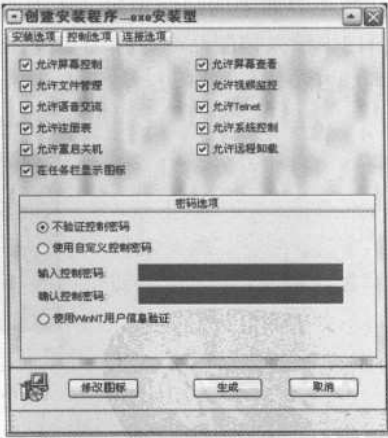
【图9-38】黑洞程序主界面

『案例9-15』创建“黑洞”服务器端安装程序。

- (1) 单击“文件→创建EXE安装版本服务端程序”，打开“创建安装程序”对话框。
- (2) 在“安装选项”中设置服务器程序的安装信息，如程序名、服务名等，如图9-39所示。
- (3) 在“控制选项”中设置允许黑洞客户端进行的控制操作，图9-40所示。



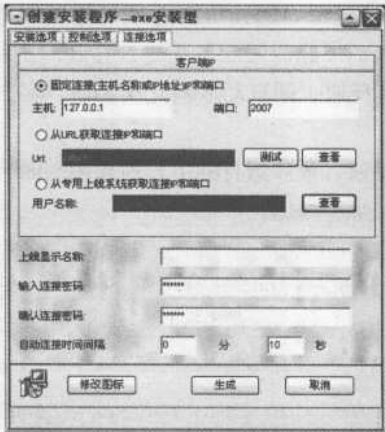
【图9-39】创建服务端安装程序



【图9-40】设置“控制选项”

(4) 在“连接选项”中设置客户端信息及连接密码等信息，如图9-41所示。如果选择“从URL获取连接IP和端口”或者“从专用上线系统获取连接IP和端口”，能够实现隐藏真正的控制端；在服务端看来，与之相连接的是我们指定的IP地址和端口。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图9-41】设置“连接选项”

(5) 单击“生成”按钮，保存设置。黑洞允许用户自定义生成的服务端程序文件名，由于文件名不规范，杀毒软件查找起来就更麻烦一些。
当目标机器运行了生成的服务端木马程序后，便可以通过黑洞2007来控制对方了。

【案例9-16】使用黑洞2007的Telnet功能。

该功能类似于Windows系统的字符终端，能够直接通过命令行方式控制对方机器。
选择主界面中的在线主机，单击命令按钮区的“Telnet”按钮，即可在打开的“字符终端”窗口中输入控制命令，作为实例，这儿在“字符终端”窗口中输入ipconfig命令，执行结果如图9-42所示：



【图9-42】黑洞2007字符终端

【案例9-17】清除黑洞2007。

手工清除：

(1) 更改注册表：

- a. 将HKEY_CLASSES_ROOT\txtfile\shell\open\command下的默认键值由S_SERVER.EXE %1更改为C:\Windows\NOTEPAD.EXE %1；
- b. 将HKEY_LOCAL_MACHINE\Software\CLASSES\txtfile\shell\open\command下的默认键值由 S_SERVER.EXE %1更改为C:\Windows\NOTEPAD.EXE %1；

- c. 将HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\下的串值Windows删除；
- d. 将HKEY_CLASSES_ROOT和HKEY_LOCAL_MACHINE\Software\CLASSES下的Winvxd主键删除。

其实只要做完前三步就算成功清除了黑洞2001，但完美的做法是将Winvxd也删除，这样做不仅可以减少注册表体积，同时也“环保”。

(2) 删除文件

到C:\Windows\SYSTEM下，删除Windows.exe和S_Server.exe这两个木马文件。要注意的是如果已经中了黑洞2001，那么Windows.exe在Windows环境下是无法直接删除的，这时可以在DOS方式下将它删除，或者用前面介绍的Windows优化大师的“进程管理”功能终止Windows.exe这个进程，然后删除。

使用软件：

这里推荐用木马克星。如果已经中了黑洞2007，运行木马克星，它会提示发现了黑洞2007。并将C:\Windows\SYSTEM下的Windows.exe改名为Windows.exe_iparmor，同时将Windows.exe这个进程关闭，重新启动机子，就将黑洞2001清除了，文件关联功能也恢复了正常。但改名后的Windows.exe_iparmor和S_Server.exe仍然在C:\Windows\SYSTEM下，为了安全起见，将它们都删除吧。由于木马克星没能将Winvxd主键删除，因此还要自己动手删除，采用方法一中的步骤4即可。

9.3.4 灰鸽子

灰鸽子是国内一款著名后门。比起前辈冰河、黑洞来，灰鸽子可以说是国内后门的集大成者。其丰富而强大的功能、灵活多变的操作、良好的隐藏性使其他后门都相形见绌。客户端简易便捷的操作使刚入门的初学者都能充当黑客。当使用在合法情况下时，灰鸽子是一款优秀的远程控制软件。但如果拿它做一些非法的事，灰鸽子就成了很强大的黑客工具。

与冰河、黑洞相同，灰鸽子软件分为客户端和服务端两部分，客户端程序运行主界面如图9-43所示：



【图9-43】灰鸽子客户端程序主界面



灰鸽子也是利用客户端程序配置出服务端程序。可配置的信息主要包括上线类型（如等待连接还是主动连接）、主动连接时使用的公网IP（域名）、连接密码、使用的端口、启动项名称、服务名称、进程隐藏方式，使用的壳，代理，图标等等，如图9-44所示。



【图9-44】配置“灰鸽子”服务端

连接密码的设定使得灰鸽子服务端程序只能被配置它的黑客控制，避免了黑客之间的竞争。

服务端对客户端连接方式有多种，使得处于各种网络环境的用户都可能中毒，包括局域网用户（通过代理上网）、公网用户和ADSL拨号用户等。

设置完成后，单击“生成服务端”按钮，即可在指定路径下生成灰鸽子的服务端安装程序。将该服务端程序植入目标主机，用户运行后就可以通过灰鸽子客户端程序控制该主机了。

灰鸽子能实现的远程控制功能包括：

- 对远程计算机文件管理：模仿Windows 资源管理器，可以对文件进行复制、粘贴、删除，重命名、远程运行等,可以上传下载文件或文件夹,操作简单易用；
- 远程控制命令：查看远程系统信息、剪切板查看、进程管理、服务管理、共享管理、代理服务；
- 捕获屏幕：不但可以连续捕获远程电脑屏幕，还能把本地的鼠标及键盘动作传送到远程实现实时控制功能；
- 视频语音，可以监控远程控制头，还有语音监听和发送功能，可以和远程主机语音对话；
- telnet（超级终端）；
- 注册表模拟器：远程注册表操作就像操作本地注册表一样方便；
- 命令广播：可以对自动上线主机进行命令播，如关机、重启、打开网页，筛选符合条件的主机等，点一个按钮就可以让N台机器同时关机或执行其它操作；
- 服务端以服务启动，支持发送多种组合键，可以轻松管理远程服务器；
- 用的自动上线系统，直接使用灰鸽子注册ID即可实现远程服务端自动上线；
- 多种自动上线方式：专用上线、DNS解析域名、固定IP等，用户自由选择。

【案例9-18】清除灰鸽子。

清除灰鸽子要在安全模式下操作，主要有两步：清除灰鸽子的服务，和删除灰鸽子程序文件。

(1) 清除灰鸽子的服务

2000／XP系统：

- a、打开注册表编辑器（点击“开始”→“运行”，输入“Regedit.exe”，确定。），打开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services注册表项。
- b、点击菜单“编辑”→“查找”，“查找目标”输入“game.exe”，点击确定，我们就可以找到灰鸽子的服务项（此例为Game_Server）。
- c、删除整个Game_Server项。

98／me系统：

在9X下，灰鸽子启动项只有一个，因此清除更为简单。运行注册表编辑器，打开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run项，我们立即看到名为Game.exe的一项，将Game.exe项删除即可。

(2) 删除灰鸽子程序文件

删除灰鸽子程序文件非常简单，只需要在安全模式下删除Windows目录下的Game.exe、Game.dll、Game_Hook.dll以及Gamekey.dll文件，然后重新启动计算机。灰鸽子VIP 2005服务端已经被清除干净。

9.3.5 Windows自带网络远程控制

Windows自带的网络远程控制工具，即远程桌面，主要包括客户端和服务端，每台Windows主机都同时包括客户端和服务端，也就是说它既可以当成客户端来连到别的装了Windows的机器并控制他它，也可以把自己当成服务器端，让别的电脑来控制自己。

要使用远程桌面，首先要设定登录密码，没有密码是不能进行远程桌面连接的，不然任何人都可以操作你的电脑，那岂不是完蛋。

【案例9-19】为用户设置登录密码。

- (1) 单击“开始”→“设置”→“控制面板”命令，如图9-45所示，打开“控制面板”。



【图9-45】打开控制面板

- (2) 在“控制面板”中双击“用户账户”，如图9-46所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图9-46】选择“用户账户”

(3) 在“用户账户”中选择要设置密码的用户，单击“创建密码”链接，如图9-47所示。



【图9-47】创建密码

(4) 输入并确认密码后，单击“创建密码”按钮即可。至此，密码创建完成，关闭“控制面板”返回桌面。接下来就要更改远程桌面设置。

『案例9-20』更改“远程桌面”设置。

(1) 右键单击“我的电脑”图标，选择“属性”菜单，如图9-48所示，打开“系统属性”对话框。



【图9-48】“我的电脑”属性

(2) 选择“远程”选项卡，选中“允许用户远程连接到此计算机”前面的复选框，如图9-49所示，单击“确定”，远程桌面设置完成。



【图9-49】远程桌面设置

完成了设置时候就可以创建远程桌面连接了。

【案例9-21】创建远程桌面连接。

(1) 打开“远程桌面连接”对话框，在“计算机”中输入目标计算机名或IP地址，如图9-50所示。



【图9-50】远程桌面连接

(2) 单击“连接”按钮，屏幕上出现“登录到Windows”对话框，如图9-51所示。



【图9-51】“登录到Windows”对话框

(3) 在“登录到Windows”对话框中输入用户名和密码，单击“确定”，远程桌面连接成功。操纵连接后的界面和本地桌面没什么分别，只是在顶部多了一个浮动的工具条，其中显示远程连接的电脑的名称或IP地址，如图9-52所示。



【图9-52】远程桌面连接成功

9.4 小结

本章介绍了木马的功能、分类、隐藏方式及启动方法，演示了几款网络中广泛流传的远程控制工具，并讲述了查杀木马的方法。

大家通过本章的学习，应该了解常用远程控制软件的使用，并且要明白一点：远程控制工具和木马并非同一概念。远程控制软件本身并没有善恶之分，它们被善意的使用者使用时就是功能非常强大的管理工具；而如果被恶意的用户使用，就成了危害网络的木马。希望大家不要以入侵他人电脑窥探隐私、破坏资源等为目的使用这些工具，做一个正义的黑客。

第10章 局域网黑客工具

局域网是计算机网络的重要组成部分，自20世纪70年代末，因微型计算机价格不断下降获得了日益广泛的使用，促使计算机局域网技术得到了飞速发展，并在计算机网络中占有非常重要的地位。

本章从局域网基础知识入手，重点讲述局域网黑客工具以及局域网安全保护常用的方法。在本章最后是对无线局域网的简单介绍，它正日益受到人们的关注。

本章要点

- ◎ 了解局域网的基础知识，及存在的安全隐患
- ◎ 掌握常用局域网密码探测工具的使用方法
- ◎ 掌握局域网控制工具的使用方法
- ◎ 了解常用局域网攻击工具
- ◎ 了解无线局域网及安全防护

10.1 局域网安全介绍

不要认为自己在局域网中，不会有黑客来攻击，黑客也不会对个人计算机产生兴趣。其实这种想法大错特错了，很多人都是抱着好奇的心理，运行黑客软件。而首先遭殃的就是局域网中的邻居。所以了解局域网安全方面的常识，对保护个人计算机是很有必要的。下面先来看看局域网相关的基础知识。

10.1.1 局域网基础知识介绍

1. 什么是局域网

局域网（Local Area Network，简称LAN），又称局部区域网，是指局限于相对小的空间，如一栋建筑甚至一间办公室内，由计算机和其他数字通信设备构成的网络。

2. 局域网的主要特点是：

- 网络范围较小，且地理范围和站点数目均有限。
- 传输速率较高，时延较低，常见的速率为10Mbit/s和100Mbit/s，干线网络一般采用1000Mbit/s的以太网。
- 传输质量好，误码率低。
- 支持传输介质种类多。

3. 局域网的基本组成

局域网一般由服务器，用户工作站，传输介质，网络适配器和联网设备五个部分组成。

·服务器

运行网络操作系统，提供硬盘、文件数据及打印机共享等服务功能，是网络控制的核心。目前常见的NOS主要有Netware，Unix和Windows NT三种。

·用户工作站

可以有自己的操作系统，独立工作；通过运行工作站网络软件，访问服务器共享资源，常见有DOS工作站，Windows95工作站。

·传输介质

目前常用的传输介质有双绞线，同轴电缆，光纤等。

·网络适配器

即网卡，一台独立计算机通常都不是必须配备网卡，但在构成LAN时，则是不可少的部件。

·联网设备

将工作站式服务器连到网络上，实现资源共享和相互通信，数据转换和电信号匹配的各种连接设备，如DB-15插头座、RJ-45插头座等。

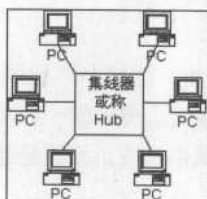
具备了以上五个构件，就可以搭建一个基本的LAN硬件平台。再运行网络操作系统（Network Operation System，NOS），局域网就能真正发挥网络互联功能，实现资源共享了。

4. 局域网的拓扑结构

网络拓扑结构是指用传输媒体互连各种设备的物理布局。目前大多数LAN使用的拓扑结构有三种：星形拓扑结构、环形拓扑结构和总线型拓扑结构。

·星形拓扑结构

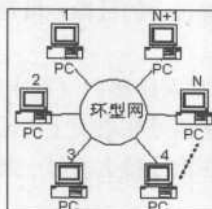
星形拓扑结构是最古老的一种连接方式，以集线器（英文名为Hub）为中心，向四周扩散，结构如图10-1所示。这种结构便于集中控制，因为端用户之间的通信必须经过中心站。但这种结构非常不利的一点是中心系统一旦损坏，整个系统便瘫痪。



【图10-1】局域网星形拓扑结构

·环形拓扑结构

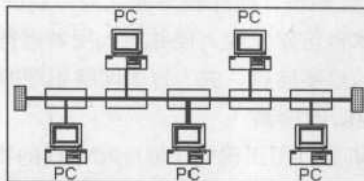
环形结构在LAN中使用较多。这种结构中的传输媒体从一个端用户到另一个端用户，直到将所有端用户连成环形。环形结构的特点是，每个端用户都与两个相邻的端用户相连，因而存在着点到点链路，但总是以单向方式操作。如图10-2所示。



【图10-2】环形拓扑结构

·总线拓扑结构

总线结构是使用同一媒体或电缆连接所有端用户的一种方式，也就是说，连接端用户的物理媒体由所有设备共享，如图10-3所示。



【图10-3】总线拓扑结构

10.1.2 局域网安全隐患

一般来说，局域网的安全主要包括两个方面，一是防黑客，二是反病毒。黑客不仅喜欢入侵单台计算机，更喜欢同时入侵到整个网络。他们能漂亮地绕过当前像防火墙之类的保护机构。

关于反病毒的问题，局域网用户尤其应该予以重视。很多公司内部局域网的用户都有这样的错误想法——他们认为既然有网管在，自己就不必在机器上装什么杀毒软件了，网管自然会把这些病毒挡在网络之外。这显然很可笑，因为网管身上并没有免疫病毒的基因，即便有，那么多病毒也挡不过来。

1. 黑客与局域网络监听技术

由于局域网中采用广播方式，因此，在某个广播域中可以监听到所有的信息包。而黑客通过对信息包进行分析，就能获取局域网上传的一些重要信息。事实上，很多黑客入侵时都把局域网扫描和侦听作为最基本的步骤和手段，原因是想用这种方法获取想要的密码等信息，这就存在很大的安全隐患。

但另一方面，我们对黑客入侵活动和其它网络犯罪进行侦查、取证时，也可以使用网络监听技术来获取必要的信息。因此，了解以太网监听技术的原理、实现方法和防范措施就显得尤为重要。

（1）在局域网实现监听的基本原理

目前很流行的以太网协议工作方式是：将要发送的数据包发往连接在一起的所有主机，包含应该接收数据包主机的正确地址，只有与数据包中目标地址一致的那台主机才能接收。但是，当主机工作监听模式下，无论数据包中的目标地址是什么，主机都将接收（当然只能监听经过自己网络接口的那些包）。

传输数据时，包含物理地址的帧从网络接口（网卡）发送到物理的线路上，如果局域网是由一条粗缆或细缆连接而成，则数字信号在电缆上传输，能够到达线路上的每一台主机。当使用集线器时，由集线器再发向连接在集线器上的每一条线路，数字信号也能到达连接在集线器上的每一台主机。

当数字信号到达一台主机的网络接口时，正常情况下，网络接口读入数据帧，进行检查，如果数据帧中携带的物理地址是自己的或者是广播地址，则将数据帧交给上层协议软件，否则就将这个帧丢弃。对于每一个到达网络接口的数据帧，都要进行这个过程。然而，当主机工作在监听模式下，所有的数据帧都将被交给上层协议软件处理。因此，如果用户的账户名和口令等信息也以明文的方式网上传输，而此时一个黑客或网络攻击者正在进行网络监听，只要具有初步的网络和TCP/IP协议知识，便能轻易地从监听到的信息中提取出感兴趣的部分。同理，正确的使用网络监听技术也可以发现入侵并对入侵者进行追踪定位，在对网络犯罪进行侦察取证时获取有关犯罪行为的重要信息，成为打击网络犯罪的有力手段。

（2）对可能存在的网络监听的检测

对于怀疑运行监听程序的机器，用正确的IP地址和错误的物理地址Ping，运行监听程序的机器如果不再次反向检查的话，就会响应。而正常的机器不接收错误的物理地址。此外，使用反监听工具也能进行检测。

另一种方法是向网上发大量不存在的物理地址的包，由于监听程序要分析和处理大量的数据包会占用很多的CPU资源，这将导致性能下降。通过比较前后该机器性能加以判断。这种方法难度比较大。

2. 局域网也是病毒高发区

如果是在多年前，局域网还是非常安全的，早期的网络攻击和恶意入侵主要来自外网，而且是少部分学习黑客技术的人所为，因此当时哪怕只是通过一个防火墙简单的封堵一些端口，检测一些特征数据包就能实现内网的安全。但是现在为了获得一些非正当的利益，很多病毒开发者打起了局域网的主意。

自冲击波病毒开始，病毒在局域网疯狂传播所造成的强大杀伤力开始让用户心惊胆战，之后计算机病毒更是控制住大量的“僵尸”电脑对特定网站或者服务器发动洪水攻击，进入2006年，网吧行业最严重的安全问题变成了ARP和DDOS，这些恶意程序不仅巧妙伪装而且无处不在，更严重的是一旦局域网某台计算机感染了病毒，就会造成大量的计算机掉线甚至整个网络陷入瘫痪，令网吧业主和网吧玩家万般无奈，在公司企业内部网络也几乎存在同样的问题，而此时传统的防火墙却显得毫无办法。

由于网游的热火而产生了ARP病毒。这是一种欺骗性质的病毒，虽然它的目的并不是破坏局域网，但为了达到它盗号盗宝的目的，会严重影响其它局域网用户的正常上网活动。所谓ARP攻击其实就是内网某台主机伪装成网关，欺骗内网其他主机将所有发往网关的信息发到这台主机上。但是由于此台主机的数据处理转发能力远远低于网关，所以就会导致大量信息堵塞，网速越来越慢，甚至造成网络瘫痪，而且ARP病毒这样做的目的就是为了截取用户的信息，盗取诸如网络游戏帐号、QQ密码等用户信息，因此它不仅会造成局域网堵塞，也会威胁到局域网用户的信息安全。

很多针对特殊服务器或是网游私服的DDOS攻击也开始大举利用网吧或企业网络中的客户机作为“僵尸”电脑，对指定的服务器IP发送大量的数据包，“僵尸”电脑越多，服务器被消耗的带宽也越多，利用这个原理耗尽服务器的带宽，就可以达到让对方服务器掉线以便对服务器运营者进行恶意勒索的目的。这种攻击方式虽然是针对外网服务器，但是它在攻击过程中需要向路由器发送大量的数据包，会直接导致路由器仅有的100M LAN口被“堵满”，因此其他局域网的计算机的请求无法提交到路由器进行处理，结果就产生局域网计算机全部“掉线”的现象。

还有一种针对服务器的SYN攻击也会令局域网电脑全体“掉线”：SYN攻击属于DOS攻击的一种，它利用TCP协议三次握手的等待确认缺陷，通过发送大量的半连接请求，耗费CPU和内存资源。SYN攻击除了能影响主机外，还可以危害路由器、防火墙等网络系统，事实上SYN攻击并不管目标是什么系统，只要这些系统打开TCP服务就可以实施。配合IP欺骗、SYN攻击能达到很好的效果，通常，感染SYN病毒的客户端在短时间内伪造大量不存在的IP地址，向服务器不断地发送SYN包，服务器回复确认包，并等待客户的确认，由于源地址是不存在的，服务器需要不断的重发直至超时，这些伪造的SYN包将长时间占用未连接队列，导致正常的SYN请求被丢弃，目标系统和路由器运行缓慢，严重的时候就直接引起整个局域网的网络堵塞甚至系统瘫痪。

其实对于网吧和大中型企业网络来说，关于局域网内部的管理一直是一个非常复杂和令人头痛的问题，掌握一定的技术原理对于局域网安全防范是非常有用的。但是，这不代表不懂这些技术，面对网络攻击就会束手无策。事实上，很多网络防护软件开发商也在产品中加入了相关技术，只要学会使用软件工具，即使没有专业的网络知识，也能轻松成为局域网黑客高手。从下一节开始，就将详细介绍一些常用的局域网攻击和防护软件的使用方法。

10.2 局域网密码探测工具

密码破解，永远是黑客研究的主题，本节我们介绍几种局域网密码侦探工具的使用。

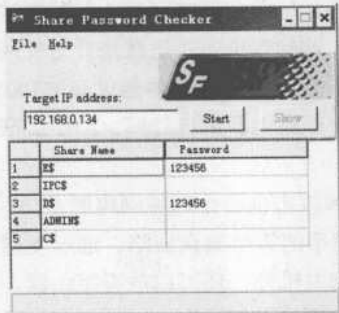
10.2.1 Share Password Checker

Share Password Checker (SPC) 是本章介绍的第一款局域网密码破解工具，专门用来破解网上邻居资源共享密码。该软件利用“Share Level Password”漏洞来破解Windows 95/98/Me系统共享密码，这个漏洞允许任意用户访问Win9x文件共享服务，即使此共享目录已经受到口令保护，攻击者并不需要知道真实口令。但是这是一款非暴力破解工具，所以如果目标机打了微软补丁就破不出了。

【案例10-1】使用Share Password Checker 查看主机共享密码。

(1) 运行Share Password Checker，在“Target IP Address”中输入目标机器的IP地址，单击“Start”按钮，立刻就能把对方机器的共享情况列举出来。

(2) 这时候的Password中显示的只是一串“*”，星号的个数表示密码的长度。此时再单击“Show”按钮，对方的密码就会显示在SPC窗口中了，如图10-4所示。



【图10-4】 Share Password Checker主界面

10.2.2 局域网络密码探测器

局域网络密码探测器是一款功能强大的局域网探测捕获工具，它可以获取局域网中任意一台电脑的账号密码，支持交换机环境下的局域网嗅探，目前支持POP3、FTP、SMTP、

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

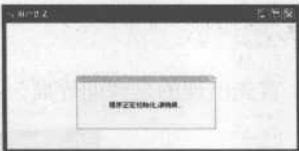
NNTP、IMAP、TELNET、HTTP、IRC 协议中的密码探测，支持 IP 转接，同时还提供众多局域网工具软件。

网络密码嗅探器在线版本，支持以下工具：

- Active Wall——局域网流量监控工具，提供详细的流量统计、流量显示功能。
- LanRule——局域网规则定义工具，规定局域网内的计算机可以进行哪些操作。
- PowerRecord——局域网开关机记录工具，记录局域网内机器的开关机情况。
- MacScan——局域网快速扫描工具，扫描局域网内 IP 地址与 MAC 地址的对应表，局域网内 Windows 机器的机器名、组名和用户名。
- HubSniff——基于集线器(HUB)组网环境下的密码嗅探器，探测中心连接设备是集线器的局域网内的重要数据帧。
- SwitchSniff——基于交换机(Switch)组网环境下的密码嗅探器，探测中心连接设备是交换机的局域网内的重要数据帧。
- DetectSniff——检测局域网内是否存在嗅探器的工具，通过检查局域网内哪些机器的网卡被设为混杂模式来判断是否可能存在嗅探器。
- DNSMonitor——监听局域网内 DNS 查询包的工具。
- KickIP——局域网 IP 冲突发生器，可以暂时断开某个 IP，实质上是一个 IP 抢占工具。
- Transfer——局域网 IP 转接工具，可以将两台原先直接通信的 IP 地址通过本机转接，便于嗅探器工作，实质是一个透明拦截局域网数据帧的间谍工具。
- LinkStop——局域网 IP 连接阻断工具，可以禁止局域网内两个 IP 地址的连接。
- TCPUDPLink——监听局域网内 TCP、UDP 数据包的工具。

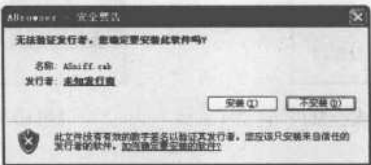
1. 安装局域网密码嗅探器

运行局域网密码嗅探器的在线版本，局域网密码嗅探器开始尝试连接到网络服务器，如图 10-5 所示。

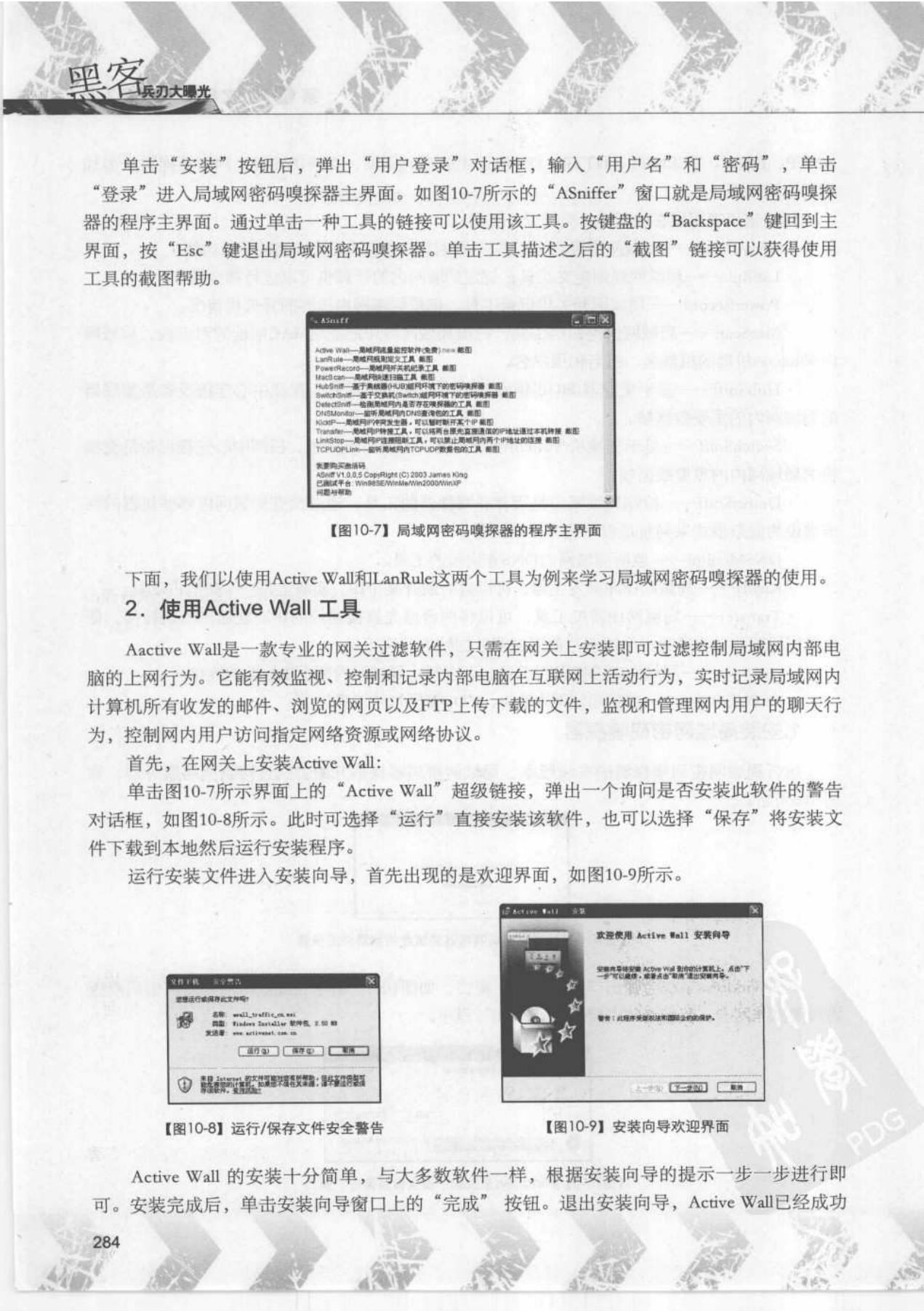


【图 10-5】局域网密码嗅探器尝试连接到网络服务器

不久 Windows 系统会弹出“安全警告”窗口，如图 10-6，由于在线版本的局域网密码嗅探器需要操作网卡，我们必须安装“ASniff.cab”程序。



【图 10-6】Windows 系统的“安全设置警告”窗口



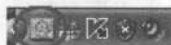
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

安装到计算机上并自动运行了。



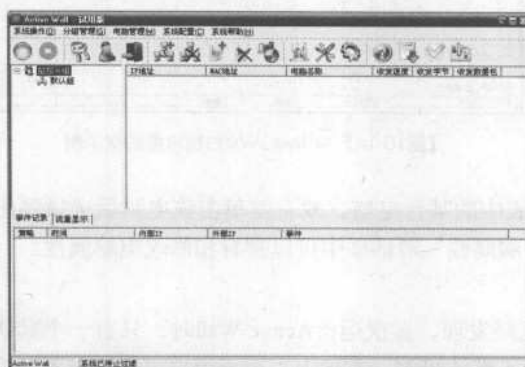
【图10-10】 Active Wall安装完成

这时，大家可以在系统工具栏里看到Active Wall 的图标，如图10-11所示。



【图10-11】 Active Wall 任务栏图标

双击Active Wall 的任务栏，在弹出的“用户登录”窗口中输入用户名和密码，登录后弹出“Active Wall”主界面，如图10-12所示。



【图10-12】 Active Wall 工具主界面

登录成功后，就可以使用Active Wall了。Active Wall最基本的功能之一是电脑管理，利用它可以将电脑增加到局域网中，或者从局域网中删除电脑，还可以对电脑进行分组管理。下面，我们就来学习怎样使用Active Wall 工具。

【案例10-2】使用Active Wall工具管理局域网中的电脑。

增加电脑

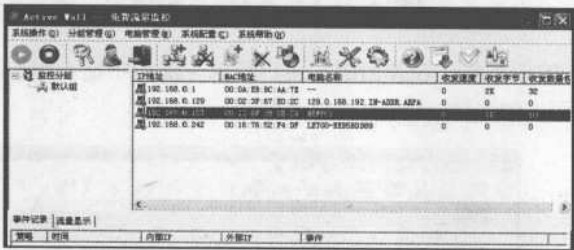
(1) 选择“电脑管理”→“增加电脑”菜单或单击工具栏上的“增加电脑”按钮，在弹出的“增加电脑”对话框中设置将要添加的电脑的属性。

我们新加入一台电脑到默认组中，IP和MAC地址分别为192.168.0.157和00:13:8F:2E:0B:C4，选择默认分组并取名为“NEWPC1”。这里的IP地址可以是局域网IP地址段中任意一个空闲IP，而MAC地址对应的是我们要添加进来的电脑的MAC地址，电脑的名字当然可以任意取，但通常都是有一定含义，以便管理，如图10-13所示。



【图10-13】Active Wall增加电脑

(2) 确认属性填写正确之后，单击“确定”按钮，新电脑就被添加到局域网中了。这时可以选择“电脑管理”→“扫描网络”菜单查看网络上的电脑，如图10-14所示。在列表中看到刚才添加的电脑“NEWPC1”及其属性。



【图10-14】Active Wall扫描电脑结果示例

(3) 双击电脑列表中的某台电脑，或右键单击该电脑后选择弹出菜单中的“电脑属性”菜单项，在弹出的“电脑属性”对话框中可以查看和修改电脑属性。

增加分组

细心的读者可能已经发现，首次运行Active Wall时，只有一个默认分组，刚才我们新增加的电脑，自动被添加到了默认组中。实际上，由于用户可能拥有不同的权限，这时，需要将他们划分到不同的组里面分别进行管理。

增加分组的方法与增加电脑相似，具体的操作步骤如下：

- (1) 选择“分组管理”→“增加分组”菜单，或是单击工具栏上的“增加分组”按钮，打开“增加分组”对话框，输入分组名后单击“确定”按钮即可。
- (2) 添加完成后在“监控分组”下就会显示新增加的分组名称。同样的，可以通过双击分组名或右键单击分组选择“分组属性”按钮，修改分组名称。
- (3) 新的分组添加到局域网后，该分组中还没有电脑，通过鼠标拖动电脑列表中的电脑到目标分组，或在“电脑属性”对话框中为电脑选择新的分组，这两种方法都可以将电脑添加到新的分组中。增加分组后的效果如图10-15所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图10-15】Active Wall增加分组

删除分组/电脑

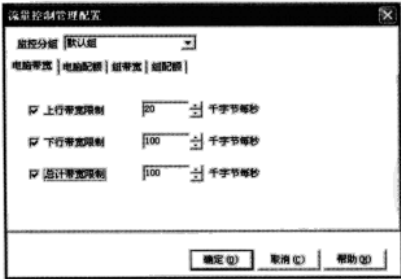
当需要从局域网中删除某个分组或某台电脑时，分别选择“删除分组”、“删除电脑”菜单项，或单击工具栏上的“删除分组”、“删除电脑”按钮即可。

注意：删除分组并不删除属于该分组的电脑，而是把这些电脑自动转移到默认组中，默认分组是不允许用户删除的；要删除网络中的电脑，只能通过“删除电脑”。

Active Wall工具的另一个重要功能是流量控制，它能够控制局域网内部每台电脑或全组的传输速度，设置网络内部每台电脑或全组每天允许的最大网络流量等。

【案例10-3】使用Active Wall 进行流量控制。

- (1) 在“监控分组”里右键选择要设置流量控制的电脑组。
- (2) 选择“策略配置”→“流量控制”快捷菜单，打开“流量控制管理配置”对话框。
- (3) 选择“电脑带宽”选项卡，选中要限制的项目，输入数值即可。该选项限制选定分组中每台电脑的网络传输速度，如图10-16所示。



【图10-16】Active Wall流量控制

- (4) “电脑配额”选项限制选定分组中每台电脑每天的总流量；“组带宽”限制所选分组所有电脑累加的传输速度；“组配额”则是限制所选分组全部电脑每天的走流量。对这几个选项的设置，读者可根据实际需要，按照步骤（3）中的方法进行，这里就不再赘述。



流量控制中，“上行带宽”表示局域网发送数据到互联网的字节数；“下行带宽”指局域网从互联网接收的字节；“总计带宽”包括上行和下行的累加字节。分组带宽以千字节每秒为单位。“配额”指的是每天允许的最大网络流量，以兆字节每天为单位。

Active Wall还有一个非常强大且实用的功能，那就是过滤。目前最新版本可以支持“MAC地址过滤”、“IP地址过滤”、“DNS过滤”、“HTTP过滤”、“SMTP过滤”、“POP3过滤”、“即时聊天过滤”、“FTP过滤”等，还能够防止用户使用P2P工具占用过多带宽。下面，我们通过“即时聊天过滤”来学习使用Active Wall的过滤功能。

【案例10-4】使用Active Wall进行“即时聊天过滤”。

- (1) 右键选择要进行“即时聊天过滤”的电脑分组，在弹出的快捷菜单中选择“策略配置”→“即时聊天过滤”选项，打开“即时聊天过滤”对话框。
- (2) 在文本域中选择要设置过滤的聊天工具，然后在“策略”下拉列表框中选择应用于该聊天工具的策略，单击“更新”按钮，文本域中对应工具的策略就会立刻变成我们刚才设置的策略。软件提供了四种可供选择的策略，分别是：“通过”、“拦截”、“通过并记录”、“拦截并记录”。
- (3) 按照同样的方法对所有需要设置过滤的聊天工具进行设置，完成之后单击“确定”按钮，Active Wall 就会按照所做的设置工作了。如图10-17中，把QQ、网易泡泡和迅雷这三个工具设置成为“拦截”，这样，所选分组中的电脑用户就不能使用这几个工具。



【图10-17】Active Wall即时聊天过滤

事实上，Active Wall的功能还有很多，例如网络身份验证——要求用户输入正确账号和密码后才可访问互联网，且支持多种验证方式；代理转发——可以与普通的代理服务器配合实现透明代理服务，而无需在客户端作任何代理设置；告警信息通知、日志输出、网关杀毒、垃圾邮件处理等等。

3. 使用LanRule工具

LanRule是一款局域网规则定义工具，功能包括绑定局域网内的Mac和IP地址、禁止某台计算机不能上网、禁止访问某个IP地址、禁止除了http、pop3、smtp之外的tcp连接、禁止使用ICQ、QQ连接等。

单击局域网密码嗅探器主界面上的“LanRule”链接，打开“LanRule”窗口，如图10-18所示。通过LanRule我们可以任意编辑局域网的通信规则，规则编辑格式可以单击“示例”查看。



【图10-18】LanRule运行界面

【案例10-5】使用LanRule工具绑定MAC和IP地址。

在规则定义文本框中输入下面这个命令：

```
if SrcMac="00:16:76:52:F4:DF" and SrcIP<>"192.168.0.2" then KickMacIP SrcMac,SrcIP
```

单击“开始执行”按钮，LanRule就按照该命令定义的规则运行，将IP（192.168.0.2）与MAC地址（00:16:76:52:F4:DF）绑定。

在上面定义的这个规则下，MAC地址为00:16:76:52:F4:DF的电脑只能使用192.168.0.2这个IP地址上网，如果是XP系统的用户想通过手动配置指定其他IP地址，系统会提示他所指定的IP地址已经被使用，而不会将这个分配给该用户。

【案例10-6】使用LanRule工具禁止某台电脑上网。

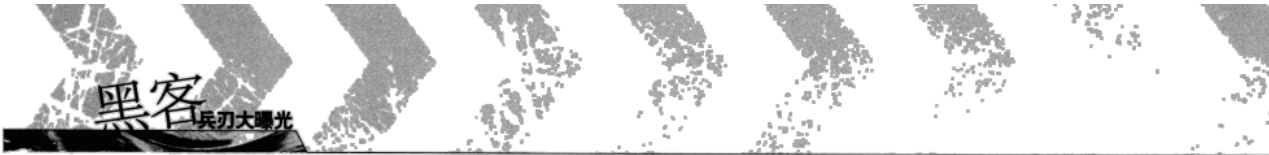
在规则定义文本框中输入命令：

```
if SrcIP="192.168.0.2" then StopIP SrcMac,SrcIP,"192.168.0.1"
```

其中，SrcIp是禁止上网的电脑所使用的IP地址，“192.168.0.1”是网关地址。单击“开始执行”按钮，IP为“192.168.0.2”的这台计算机就不能访问网络了。



实际使用LanRule时可以同时将多个命令结合起来使用，如：同是执行前面两个案例中的命令，就可以让命令中指定的MAC地址对应的计算机，使用任何一个IP地址都无法访问网络，从而彻底禁止了该计算机上网。



10.2.3 局域网QQ号码嗅探器

局域网QQ号码嗅探器V1.0只能在支持RAW SOCKET的机器上运行，而且还得是非交换机的局域网内，它可以嗅到整个局域网内的QQ号码。该版本QQ号码嗅探器运行后的界面如图10-19所示。



【图10-19】QQ号码探测器主界面

运行QQ嗅探器后单击“开始监听”按钮，即可开始探测整个局域网中的QQ号码和它登录的IP地址，并将探测到的结果显示在界面上左边的空白窗口中。

1. QQ Sniffer

QQ Sniffer 是基于交换机/HUB环境下QQ号码嗅探工具，只在本机运行，不管是否开了共享，也不需要事先在远程计算机安装服务端。目前QQ Sniffer已经发展到2007 build 3版。该软件主要有四个功能：

- 监听网吧在线QQ号码；
- 使指定计算机无法上网；
- 制造IP冲突；
- 强制和某个QQ聊天。

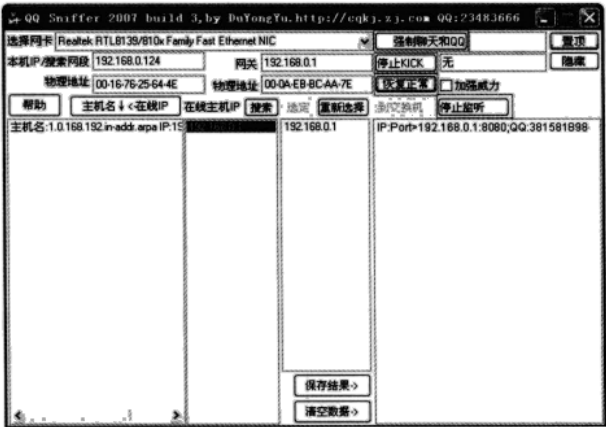
【案例10-7】使用QQSniffer探测局域网中的QQ号码。

(1) 登录，运行QQSniffer.exe文件，首先出现一个“Help and About”窗口，该窗口除详细介绍了QQSniffer的相关信息外，还要求用户在此登录，如图10-20所示。QQSniffer可以接受QQ号码和网易邮箱两种登录方式，使用163邮箱是2007 build 3版新增加的功能。



图10-20】QQSniffer帮助和关于界面

- (2) 设置，填写好登录信息后单击“登录”按钮即可使用QQSniffer。首先要设置网卡类型和本机的IP及MAC地址。软件会自动搜索本机网卡以及网络地址信息，将其列入选择网卡旁的下拉列表框中（多网卡环境下列表框中会有多个选项），用户只需通过下拉列表选择正确的网卡即可。
- (3) 单击“搜索”按钮搜索网络中所有在线的计算机，搜索结果显示在“在线主机IP”列表框中。
- (4) 在“在线主机IP”列表框中选择要操作的IP地址，按“选定”按钮，结果显示在右边的列表框中。可以选择一个或多个主机IP。如果要重新选择，单击“重新选择”按钮。
- (5) 选择主机后单击“开始监听”得到所选IP计算机上在线的QQ号码，结果显示在最右边的列表中。图10-21是一个监听局域网中QQ号码的示例，其中QQ号码列表中的数据分为两个字段：前面是所监听的计算机的IP地址和端口，后面是得到的QQ号码。



【图10-21】执行指定功能后的界面

除了监听网络中在线QQ号码外，QQSniffer还可以在网络中制造IP冲突，使某个QQ号码掉线以及强制和某个QQ聊天的功能，该软件操作起来也十分简单，用户只需在选定主机之后单击不同的按钮。

主界面上的四个按钮：“监听QQ号码”、“掉线”、“IP冲突”和“强制聊天和QQ”分别对应QQSniffer的四个主要功能。前三项功能开始执行后，它们所对应的按钮分别变为：“停止监听”、“恢复正常”和“停止KICK”。“强制聊天和QQ”按钮不会变化，此时只要该按钮旁边的文本框中输入列表中搜索到的任意一个QQ号码，就可以开始与它在聊天。

10.3 局域网查看控制工具

上一节我们介绍了局域网密码探测工具，接下来就可以进行局域网中信息的查看和控制了。本节将介绍两种最常用的局域网查看和控制工具的使用。

10.3.1 LAN Explorer

伴随网络的飞速普及，越来越多的个人电脑互连组成了局域网（Lan），然后联入互联网（Internet）。局域网的规模由原来的几台、十几台，逐渐发展到现在的几十台，甚至上百台。

而与此同时，现代普及的操作系统仍然是操作简便的Windows 9x系统，局域网内资源的共享和文件传输的方式现在绝大部分是通过Windows提供的“网上邻居”服务，该服务基于NetBIOS协议。

由于“网上邻居”自身的局限性，使得在如此浩瀚的网络资源里，能够迅速找到所需要的信息变得很困难，传统的采用手工查询的方式已经不能适应人们越来越快的生活工作节奏，新的查询方式和工具已经成为一种不可阻挡的趋势。在如此巨大的需求市场和如此贫乏的服务对比之下，基于NetBIOS协议的LAN Explorer局域网搜索引擎的产生变得迫不及待。

1. LAN Explorer的特点

(1) LAN Explorer局域网搜索引擎将原来基于http、ftp等网络协议的机器人搜索算法扩展应用于NetBIOS协议之上，实现对于整个局域网的目录搜索。这一创新在全国甚至在上都是具有领先水平的，适用于通过高速网线连接的局域网。

(2) 快速高效地搜索、浏览局域网资源。多线程搜索局域网上所有的工作组、主机、打印机、共享文件。

(3) 可以按照网上邻居、工作组或者按照IP地址段自动搜索所有共享的Mp3、电影或自定义搜索的文件

(4) 内置nbtstat，能快速查找某一IP网段内的所有主机，并根据IP地址得到对方主机的主机名、工作组名、用户名、MAC地址，速度极快。能将扫描和搜索的结果保存成文本文件或excel电子表格文件。

(5) 能对某一地址范围的主机进行Ping，端口扫描操作，找出所有的WEB服务器，FTP服务器等。能向某一主机发送消息。

(6) 局域网机器间拷贝文件时，提供文件和目录的断点续传的功能。

(7) 采用类似资源管理器的界面，操作十分方便，易于推广。

(8) 支持多平台，能够在Windows9X和Windows NT、Windows 2000等使用比较广泛的操作系统上运行。

2. 使用LAN Explorer

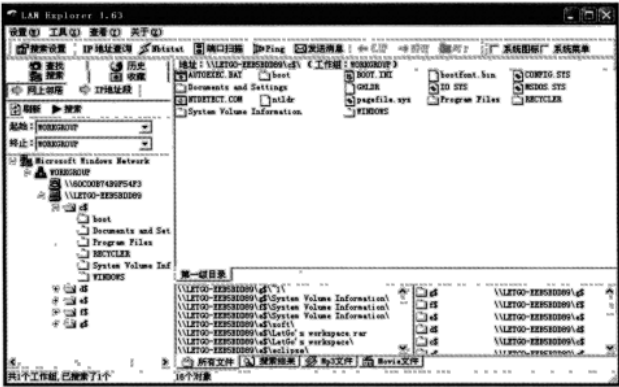
LAN Explorer最大的特点就是可以快速、高效地搜索和浏览局域网中的资源，下面还是通过实例来学习使用LAN Explorer搜索资源的方法和技巧。

【案例10-8】使用LAN Explorer搜索局域网资源。

(1) 搜索网上邻居。运行LAN Explorer，首先进入的就是“搜索”→“网上邻居”界面，如图10-22所示。图中可以看到“起始”和“终止”两个下拉列表框，供用户选择搜索范围。这里的搜索范围是按照工作组划分，可以选择某一个工作组（起始和终止条件相同）或选

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

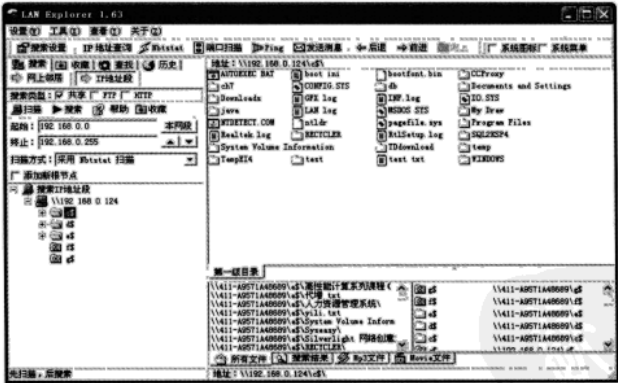
择在多个工作组中进行搜索。



【图10-22】LAN Explorer搜索网上邻居

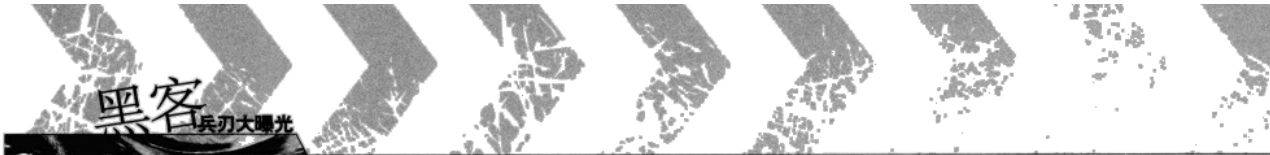
通过“网上邻居”进行搜索得到的是选定范围内在线主机的主机名，搜索结果显示在树形列表中。展开列表条目，双击其中的子项，则在右边的文件列表框中列出选定文件夹下的所有文件和子文件夹。

(2) 搜索IP地址段。选择“搜索→IP地址段”选项卡进入“搜索IP地址段”界面，如图10-23所示。在“起始”和“终止”文本框中分别输入搜索的起止IP地址范围，如果是在本网段中搜索，直接单击“本网段”，软件会自动完成IP地址段的添加。



【图10-23】LAN Explorer搜索IP地址段

设置好起始地址后先要扫描网络中的在线主机。单击“扫描”按钮，将打开“网络工具”对话框，如图10-24所示，列表框中显示了扫描的结果。这里，由于选中了该对话框状态栏上的“自动加入搜索目录树”复选框，就和搜索网上邻居相同，扫描结果会同时显示在主界面的树形列表中，不过这时的树形列表中主机节点显示的是主机IP地址。



【图10-24】LAN Explorer网络工具对话框



LAN Explorer为用户提供了三种扫描方法：采用 Nbtstat 扫描、采用 Ping 扫描和采用TCP 139 端口扫描。这三个都是探测网络连接的命令，但是采取的探测技术和侧重点有所不同。简单说来，Ping命令通常用来检查网络是否畅通或者网络连接速度；Nbtstat命令使用TCP/IP上的NetBIOS显示协议统计和当前TCP/IP连接，使用这个命令可以得到远程主机的NETBIOS信息，比如用户名、所属的工作组、网卡的MAC地址等；TCP端口扫描不仅能探测目的主机是否畅通，还能检测到端口状态。

（3）操作文件。需要注意的是，无论搜索网上邻居还是搜索IP地址段，最终的目的还是为了找到位于网络主机中的有用资源，两种搜索方式没有先后顺序，只是按不同的条件来搜索。

搜索结束后，我们可以在文件列表框中对需要的文件或文件夹进行操作。右键单击列表框中的文件或文件夹，在弹出的快捷菜单中有打开、复制、删除等操作，还可以查看文件大小及其他文件属性。利用这些菜单项，可以像操作本地文件那样操作网络主机上的文件。

（4）为了达到快速查找文件的目的，LAN Explorer还提供了“搜索设置”功能，用户可以自定义搜索的条件。如查找文件中含有某个特定字符串的文件，或者按文件类型（如MP3文件、Movie文件等）进行搜索。

【案例10-9】使用LAN Explorer查询IP地址。

在案例10-8中提到过，显示在目录树中的主机有主机名和IP地址两种方式，虽然两种方式都可以标识一台主机，用户怎么知道主机名和IP地址之间的对应关系呢？

LAN Explorer提供了通过主机名查找IP地址和通过IP地址查找对应的主机名的功能。选择工具栏上的“查询IP地址按钮”，打开“网络工具”对话框的“IP地址查询”选项（图10-3-4），该案例中我们是通过IP地址查找电脑主机名。图10-25中可以看到，状态栏上有两个单选按钮，当前选中的是“IP查主机名（域名）”，如果选择“主机名（域名）查IP”则可通过主机名查找对应的IP地址。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

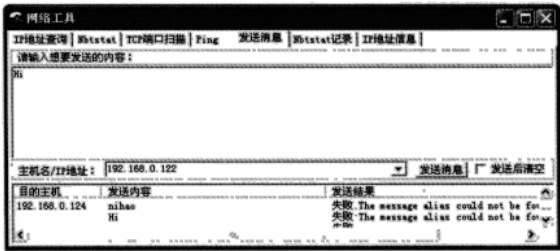


【图10-25】LAN Explorer查询IP地址

【案例10-10】用LAN Explorer 发送消息。

选择“工具→发送消息”菜单或工具栏上的“发送消息”按钮，给特定的在线主机发送消息。

在文本框中编辑想要发送的内容，然后在“主机名/IP地址”框中输入或目的主机名或IP地址，也可以从下拉列表中选择，确定目的主机后单击“发送消息”按钮就可以给网络上的主机发送消息，如图10-26所示。



【图10-26】LAN Explorer发送消息

10.3.2 NetSuper

NetSuper是一款小巧而强大的绿色软件，主要有以下功能：

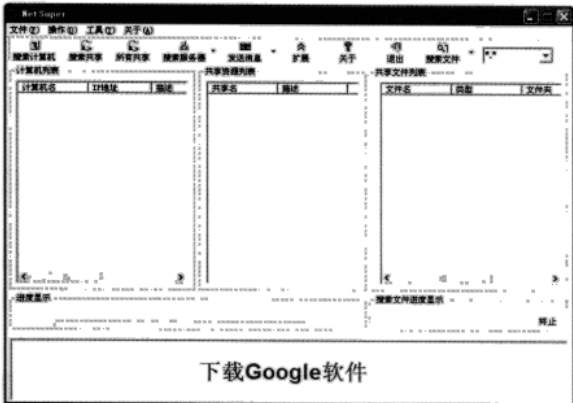
- 搜索局域网内的所有活动计算机，并显示这些计算机的IP地址，所属的域或者工作组，并显示MAC地址。
- 搜索指定的某个计算机的共享资源。
- 搜索所有计算机的所有共享资源。
- 打开某个指定的计算机。
- 打开某个指定的共享目录。
- 将某个指定的共享目录映射到本地磁盘（映射网络驱动器）。
- 将搜索到的计算机列表导出到文本文件。
- 将搜索到的共享资源列表导出到文本文件。
- 搜索SQL Server服务器，将局域网中的所有的活动的SQL Server服务器搜索出来。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



- 搜索局域网中所有的打印服务器。
- 将局域网中的所有服务器都搜索出来。
- 给指定的计算机发送消息。
- 给指定的某个域或者工作组所有的计算机发送消息。
- 发送消息时，可以指定发送的次数、选择是否匿名发送。

NetSuper的运行主界面如图10-27所示：



【图10-27】 NetSuper的运行主界面

『案例10-11』使用NetSuper的搜索局域网中的计算机。

单击工具栏上的“搜索计算机”按钮，NetSuper会自动将局域网内的活动计算机都搜索出来，并显示每个计算机的IP地址、计算机描述、所属域或工作组以及计算机的MAC地址等信息，如图10-28所示。



【图10-28】 NetSuper搜索计算机

该软件对搜索结果有自动保存功能，即软件退出时，将自动保存本次搜索的结果，再次启动该程序时能够显示上一次的搜索结果。单击列表中的字段名显示结果可以根据用户所需的字段排序。

『案例10-12』使用NetSuper的搜索局域网中的服务器。

- (1) 单击“搜索服务器”按钮，系统将自动搜索局域网中的所有服务器，并将搜索到的

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

服务器和运行的操作系统及其版本显示在服务器列表中，搜索结果如图10-29 所示。
(2) 双击搜索结果中所列出的服务器名，还可以查看服务器用户信息，如图10-30所示。

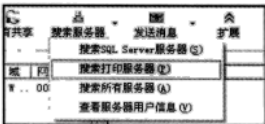


【图10-29】搜索服务器结果示例



【图10-30】服务器用户信息

(3) 如果要搜索打印服务器则单击“搜索服务器”按钮的下拉菜单，选择“搜索打印服务器”即可，图10-31所示。



【图10-31】搜索打印服务器

『案例10-13』使用NetSuper的局域网消息发送功能。

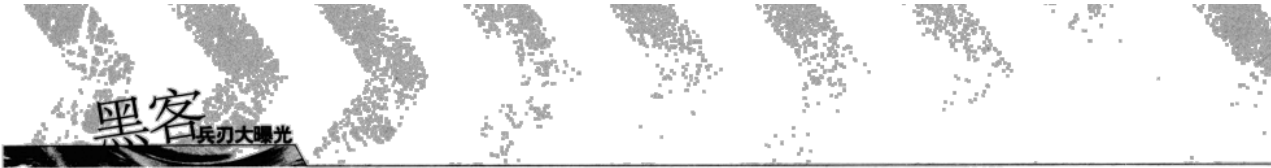
在主界面上单击“发送消息”按钮，弹出如图10-32 所示的对话框。分别填写计算机名或IP地址、消息内容、选择实名或匿名发送，单击“发送”即可将自定义的消息发送到目标机器。



【图10-32】NetSuper的局域网消息发送功能

10.4 局域网攻击工具

俗话说“知己知彼，百战百胜”。要想使自己的计算机在局域网中尽量免受黑客的恶意攻击，了解常用的局域网攻击工具是非常有必要的，这样才能采取有效的防范措施，把黑客拒之门外。



10.4.1 全自动局域网在线机器攻击机

全自动局域网在线机器攻击机的功能是让局域网中的在线机器掉线，该软件利用 WindowsXP 系统的远程关机漏洞，可以用来监测局域网内所有有漏洞的机器。用 netstat 命令查看本机端口可以发现，该工具工作时通过与目标主机建立 TCP 连接，向 139 和 445 端口发送 SYN 信号来实现攻击目，攻击结束后本机端口处于 TIME_WAIT 状态。

『案例10-13』使用局域网在线机器攻击机。

- (1) 首先单击主界面上起始IP地址旁的“本地”按钮，文本框中出现的默认起始和终止IP地址是192.168.0.1—192.168.0.254。这两个地址都可以自己指定，如果要攻击一台机器，就把起始和终止IP地址都设置为目标主机的IP。在该案例中设定攻击目标为192.168.0.253这台电脑。
- (2) 设置线程数，该数字指定了在线机器攻击机所能发起的最大线程数量，默认为40。这里使用它的默认值。
- (3) 如果选中“只攻击Ping通主机”这个选项，在攻击时就不攻击那些使用Ping命令发现不了的主机；选中“测试WinXP远程关机”，攻击机会向指定IP地址范围内的所有主机都发起攻击。
- (4) 设置完成后，单击“开始攻击”按钮，全自动局域网在线机器攻击机就会根据我们的设置自动完成攻击。如图10-33所示。



【图10-33】全自动局域网在线机器攻击机主界面

- (5) 全自动在线机器攻击机还可以指定攻击时间，选中右上角的“启用延时”复选框，可以任意制定在多少分钟以后开始攻击，延时攻击会隐藏程序界面，到时间就自动开始攻击。如图10-34所示攻击的效果。



【图10-34】攻击效果

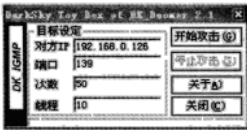
10.4.2 局域网IP炸弹

局域网IP炸弹是通过发送大量的特殊数据包给局域网中的计算机，利用Windows系统的漏洞进行攻击，以消耗100%的系统资源，导致计算机死机或重启。

IP炸弹攻击主要针对某一个IP地址段内的服务器。对Windows 95/NT来说，主要是利用NetBIOS网络协议的例行处理程序OOB的漏洞，将一些特定的数据封包，以OOB方式放在某个IP地址的某个开启的端口上（通常为139、137、135），使电脑突然死机；对Windows 98系统的攻击主要是针对Windows98系统的自身蓝屏漏洞；而对Windows 2000的攻击，是通过其本身存在很多拒绝服务的漏洞。

【案例10-14】使用IP炸弹进行攻击。

局域网IP炸弹的使用方法十分简单，在“对方IP”和“端口”文本框中输入目标机器的IP地址和端口号，指定次数和线程后单击“开始攻击”按钮，如图10-35所示。这时局域网IP炸弹就会以用户指定的线程数向目标机器的指定端口发送指定数量的数据包。数据包达到一定数量后，目标机器就会因为资源耗尽而死机，造成机器死机所需发送的数据包次数与目标机器的性能有关。



【图10-35】局域网IP炸弹界面

10.4.3 局域网终结者

网络终结者是利用构造虚假ARP包来欺骗网络主机，使得被指定的主机被迫从网络中断开来实现其攻击目的。局域网终结者只对以路由作为划分的同一局域网内主机产生作用。

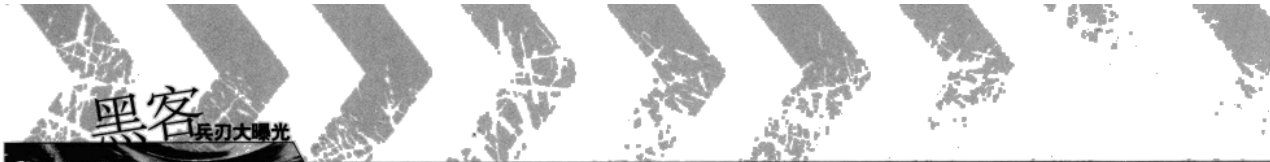
【案例10-15】使用局域网终结者进行攻击。

运行局域网终结者，在“目标IP”之后的文本框中输入目标机器的IP地址，单击“添加到阻断列表”按钮，将其加入到阻断列表中即可，如图10-36所示。



【图10-36】网络终结者程序界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



退出程序或单击“取消选中地址”按钮将目标IP从列表中移除，目标主机将在30~60秒后恢复正常工作(有的系统可能需要更长时间)。

10.4.4 EtherPeek NX获取局域网的账号密码

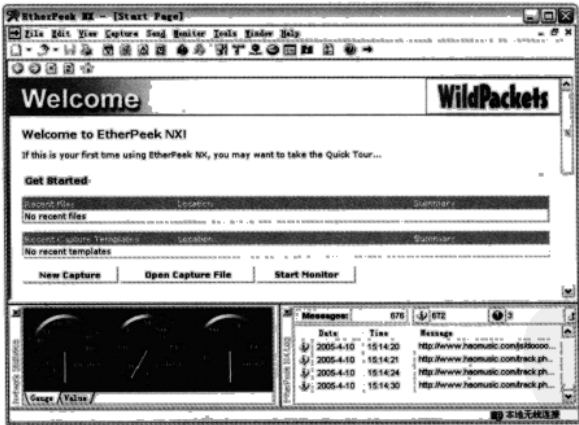
在局域网其实很容易获取用户的各种私人信息，例如登录网站或FTP服务器的用户名和密码等。要用自己的机器获取用户信息，需要满足三个条件：第一，机器网卡能够收到局域网中所有用户的数据。对于Hub级联的局域网这没有问题。对于交换机连接的局域网，可通过交换机将网卡连接的端口设置为监控（Port Monitor）模式。第二，机器网卡设置为混杂模式。第三，对于大量抓获的网络数据，需要拥有功能强大的协议分析软件。具备这三个条件后，获取局域网内用户的用户密码信息就变得易如反掌了。

【案例10-16】用EtherPeek NX获取HTTP和FTP密码。

可以使用一款协议分析功能非常强大的软件——EtherPeek NX，并利用它来获取局域网内用户的HTTP和FTP密码。

EtherPeek NX是Wild Packets公司出品的用于提供信息包捕获过程中实时专业诊断和结构解码的网络协议分析软件。EtherPeek NX是专业级的网络数据群和协议分析软件，它还可对现有网络面临的众多故障提供精确分析和定位。

EtherPeek NX的运行主界面如图10-37所示。



【图10-37】 EtherPeek NX的运行主界面

1.抓包设置

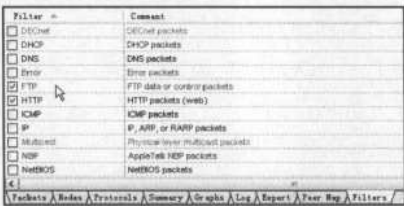
单击“Capture”→“Start Capture”命令，在弹出的“Capture Option”对话框中，选择本地网卡，将本地网卡设置为混杂模式，图10-38所示。



【图10-38】EtherPeek NX设置本地网卡

2.设置抓包过滤器

(1) 单击“Filters”标签，并选择FTP和HTTP，如图10-39所示。为了直接获得FTP和HTTP的用户密码，需要对过滤器进行高级设置。



【图10-39】EtherPeek NX设置抓包过滤器

(2) 鼠标双击“FTP”，在弹出的“Edit Filter”对话框中，单击“Protocol”按钮，在弹出窗口中找到“FTP”，选择“Control”，即只抓取FTP控制报文，并单击“OK”确认，如图10-40所示。

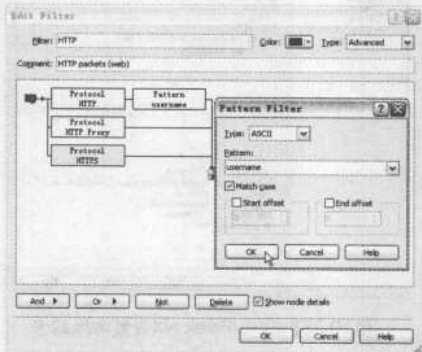


【图10-40】EtherPeek NX设置FTP高级过滤器

(3) 鼠标双击“HTTP”，在弹出的“Edit Filter”对话框中，单击“Add”按钮，选择



“Pattern”，在弹出窗口中添加“Pattern”为“username”，并单击“OK”确认，如图10-41所示。



【图10-41】EtherPeek NX设置HTTP高级过滤器

3.数据抓取

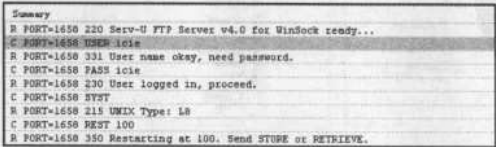
回到主界面，单击“Start Capture”按钮开始数据采集。采集一段时间后，单击“Stop Capture”按钮停止。



理论上讲，采集的时间越长，收集到的数据越多，获取局域网用户的私人信息就越多。

4.数据分析

(1) FTP的用户名和密码直接在抓包窗口主界面上的“Summary”中就可以非常直观的看到，如图10-42所示的某一次FTP会话中，FTP服务器“Serv-U”的一个用户名是“icie”，密码也是“icie”。



【图10-42】EtherPeek NX获取FTP的用户名和密码

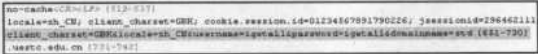
(2) 由于设置了“Pattern”，我们只抓获到少量的HTTP报文，但并非所有报文都含有用户名和密码。一般含有用户名密码信息的报文，抓包窗口“Summary”字段中应包含类似于“login.asp”、“login.jsp”、“check_login.asp”等鉴权页面的地址，如图10-43所示的三个

HTTP报文中，第一个就含有“login.jsp”。双击这个报文，打开其解码窗口。

Size	Delta Time	Protocol	Summary
740	04.068543	HTTP	C: PORT=1640: POST /login.jsp
1518	01.724412	HTTP	R: PORT=1657: HTML Data
1518	00.002554	HTTP	R: PORT=1657: HTML Data

【图10-43】找出包含用户名和密码的HTTP报文

(3) 在解码窗口中，稍微寻找一下，立即可找到一个HTTP会话的登录用户名和密码信息，如图10-44所示。



【图10-44】EtherPeek NX获取HTTP的用户名和密码

10.5 无线局域网黑客工具

近年来，随着无线局域网的高速发展，无线局域网的安全技术也得到了快速的发展和应
用。无线局域网与传统有线局域网相比优势不言而喻，它可实现移动办公、架设与维护更容易
等。下面我们来说明无线局域网的黑客工具。

10.5.1 无线局域网搜索工具

找到无线网络是攻击的第一步，这里推荐两款常用工具：

- (1) Network Stumbler。这个基于Windows的工具可以非常容易地发现一定范围内广播出
来的无线信号，还可以判断哪些信号或噪音信息可以用来做站点测量。
- (2) Kismet。NetStumbler缺乏的一个关键功能就是显示哪些没有广播SSID的无线网络。
如果将来想成为无线安全专家，你就应该认识到访问点（Access Points）会常规性地广播这个信
息。Kismet会发现并显示没有被广播的那些SSID，而这些信息对于发现无线网络是非常关键的。

【案例10-17】用Network Stumbler搜索无线信号。

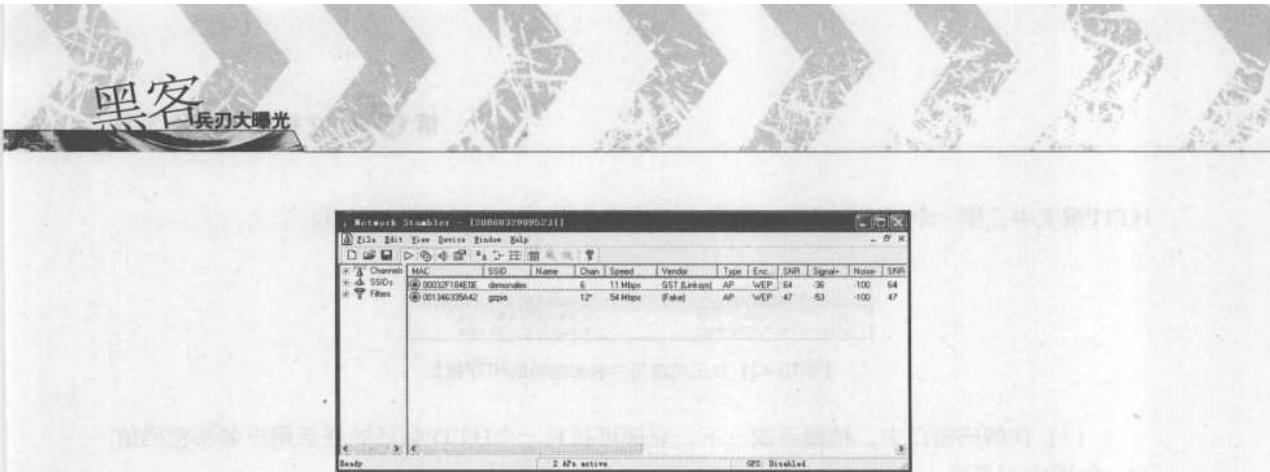
启动Network Stumbler，系统会自动的进行无线AP的搜索，搜索完毕后打开如图10-45所示
的操作界面。所搜索到的结果显示在右边的窗口中。包括MAC地址，SSID等信息。这是黑客
入侵无线网络的第一步。

红色框框部分内容确定该SSID名为“demonalex”的AP为802.11b类型设备，
“Encryption”属性为“已加密”，采用“WEP”的加密算法。



NetStumbler对任何有使用加密算法的STA“802.11无线站点”都会在
“Encryption”属性上标识为WEP算法。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图10-45】 Network Stumbler操作界面



小贴士

什么是SSID?

SSID (Service Set Identifier) 也可以写为ESSID, 用来区分不同的网络, 最多可以有32个字符, 无线网卡设置了不同的SSID就可以进入不同网络, SSID通常由AP广播出来, 通过XP自带的扫描功能可以相看当前区域内的SSID。出于安全考虑可以不广播SSID, 此时用户就要手工设置SSID才能进入相应的网络。简单说, SSID就是一个局域网的名称, 只有设置为名称相同SSID的值的电脑才能互相通信。

【案例10-18】在Cygwin系统中安装Kismet

如果说NetStumbler只是简单的检测无线网络, 那么Kismet则的确是一个无线网络嗅探器。Kismet依赖无线网卡的能力来报告数据包。幸运的是, 大多数常见的无线网卡-包括Linksys, D-Link, Cisco Aironet和Orinoco-都支持这一功能。你可以在Linux, BSD平台上或者在Windows平台上借助Cygwin的帮助安装Kismet

Kismet最初是设计运行在Linux平台上的, 如果你必须在Windows平台上运行Kismet, 也没有任何问题, 你可以安装Cygwin并在Cygwin环境下运行Kismet。

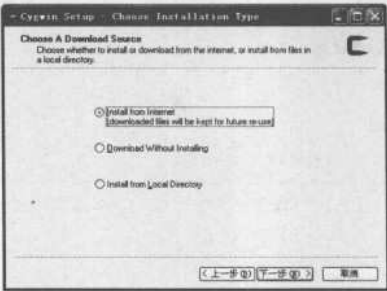
- (1) 首先到Cygwin中国官方网站下载其安装程序 (<http://www.cygwin.cn/site/install/>)。
- (2) 下载后, 双击其安装包, 弹出“Cygwin Setup”的安装界面, 如图10-46所示。



【图10-46】 “Cygwin Setup” 的安装界面

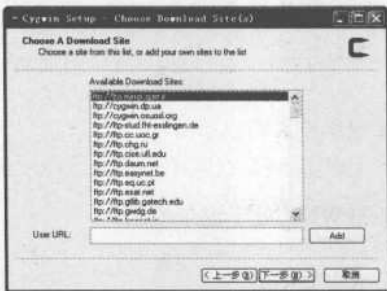
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

(2) 单击“下一步”按钮，弹出“Choose A Download Source”（选择安装资源）对话框，可以“Install from Internet”（从网络安装）的模式，如图10-47所示。



【图10-47】“Choose A Download Source”对话框

(3) 单击“下一步”按钮，选择安装的路径及文件下载的存放路径即可。然后进入“Choose A Download Site”（选择一个下载链接）的对话框中，选择要下载Cygwin安装程序的链接地址，如图10-48所示。选择下载源，你可以在下载列表里选择：<http://www.cygwin.cn>或者，直接在URL里输入<http://www.cygwin.cn/pub/>。



【图10-48】选择下载地址

(4) 安装完成后，启动Cygwin，弹出如图10-49所示的操作界面。



【图10-49】Cygwin操作界面

【案例10-19】在Liunx下安装Kismet。

如果用户是采用Liunx系统，那么可以直接在该系统下进行Kismet安装。当然了，还可以通过虚拟机的方式来安装，具体的Liunx安装的方式用户可以自己研究。

```
1.安装Kismet
#cd /usr/local/sbin
#wget http://demonalex.3322.org/download/wireless/kismet-2006-04-R1.tar.gz
#tar -zxvf kismet-2006-04-R1.tar.gz
#cd kismet-2006-04-R1
#./configure --disable-setuid
#make dep
#make && make install

2.配置Kismet
#cd /usr/local/etc
#vi kismet.conf
编辑：
suiduser=root
source=madwifi_ag,wifi0,Atheros
:wq
若需要在SHELL下使用curses模式运行的话：
#vi kismet_ui.conf
编辑：
gui=curses
:wq

3.启动Kismet
首先必须激活WNIC，然后让WNIC处于混杂模式：
#modprobe ath_pci
#ifconfig ath0 up
#wlanconfig ath0 destroy
#wlanconfig ath0 create wlandev wifi0 wlanmode monitor
最后运行kismet脚本：
#kismet
```

之后就能成功进入Kismet的操作界面，如图10-50所示。



【图10-50】Kismet的操作界面

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

从图中已经可以看到在这个覆盖区内的802.11信号源了，单击“空格键”进入主视图。

(1) 首先需要进入“选择”视图。单击“S”键，然后再单击“C”键即可使用上下按键切换各通信条目，如图10-51所示。



【图10-51】进入“选择”的视图

(3) 选中你要查看的栏目，然后单击“回车键”后，即可获取到该条目所对应的STA信息，如图10-52所示。



【图10-52】查看STA信息

(4) 单击“Q”键回到“选择”的视图，再单击“C”键，查看到该WLAN内所有的客户端的详细信息，如图10-53所示。



【图10-53】查看客户端的详细信息

(5) 分析有用的信息：

例如 AP是否启用了MAC地址访问控制列表的功能、使用MAC地址、该WLAN所使用的IP段（这类型的信息是依靠捕捉ARP包来实现的）。

在“选择”的视图下，可以通过下面的功能键来显示相应的信息：

- 【A】 显示统计信息
- 【D】 Dump出目前通信的ASCII内容
- 【R】 显示该通信的实时流量图
- 【W】 显示报警信息
- 【P】 显示802.11帧实时嗅探器

4.退出Kismet

在主视图或“选择”的视图下按“Shift+q”就可以安全退出Kismet了。

10.5.2 破解无线网络工具

发现了一个无线网络后，下一步就是努力连上它。如果该网络没有采用任何认证或加密安全措施，你可以很轻松地连上它的SSID。如果SSID没有被广播，你可以用这个SSID的名称创建一个文件。如果无线网络采用了认证和/或加密措施，也许，那么需要以下工具中进行破解。

【案例10-19】破解AirCrack进行WEP加密破解。

1.下载Win32版AirCrack程序集

(<http://www.demonalex.net/download/wireless/aircrack/WinAircrackPack.zip>)

WinAircrackPack工具包解压缩后得到一个大概4MB的目录，其中包括六个EXE可执行的文件。

- | | |
|-----------------|----------------------|
| aircrack.exe | 原WIN32版aircrack程序 |
| airdecap.exe | WEP/WPA解码程序 |
| airodump.exe | 数据帧捕捉程序 |
| Updater.exe | WIN32版aircrack的升级程序 |
| WinAircrack.exe | WIN32版aircrack图形前端 |
| wzcook.exe | 本地无线网卡缓存中的WEPKEY记录程序 |

2.捕捉信息

通过捕捉适当的数据帧进行IV（初始化向量）暴力破解得到WEP KEY，因此只需要使用airodump.exe（捕捉数据帧用）与WinAircrack.exe（破解WEP KEY用）两个程序就可以了。

（1）首先打开airodump.exe程序，按照下述操作，如图10-54所示：

①程序会提示本机目前存在的所有无线网卡接口，并要求你输入需要捕捉数据帧的无线网卡接口编号，在这里选择使用支持通用驱动的BUFFALO WNIC，编号为“26”。

②然后程序要求你输入该WNIC的芯片类型，目前大多国际通用芯片都是使用“HermesI/Realtek”子集的，因此选择“o”。

③然后需要输入要捕捉的信号所处的频道，需要捕捉的AP所处的频道为“6”。

④提示输入捕捉数据帧后存在的文件名及其位置，若不写绝对路径则文件默认存在在

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

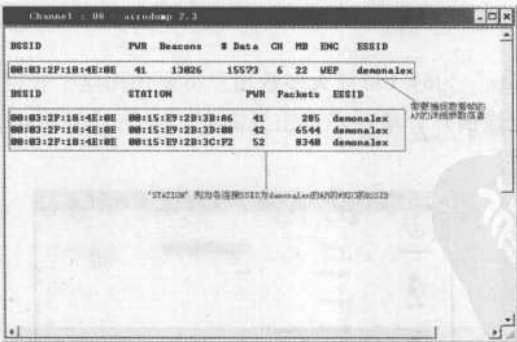
winaircrack 的安装目录下，以.cap 结尾。

⑤最后winaircrack提示：“是否只写入/记录IV[初始化向量]到cap文件中去？”，这里选择“否/n”；确定以上步骤后程序开始捕捉数据包。



【图10-54】设置ariodump.exe程序

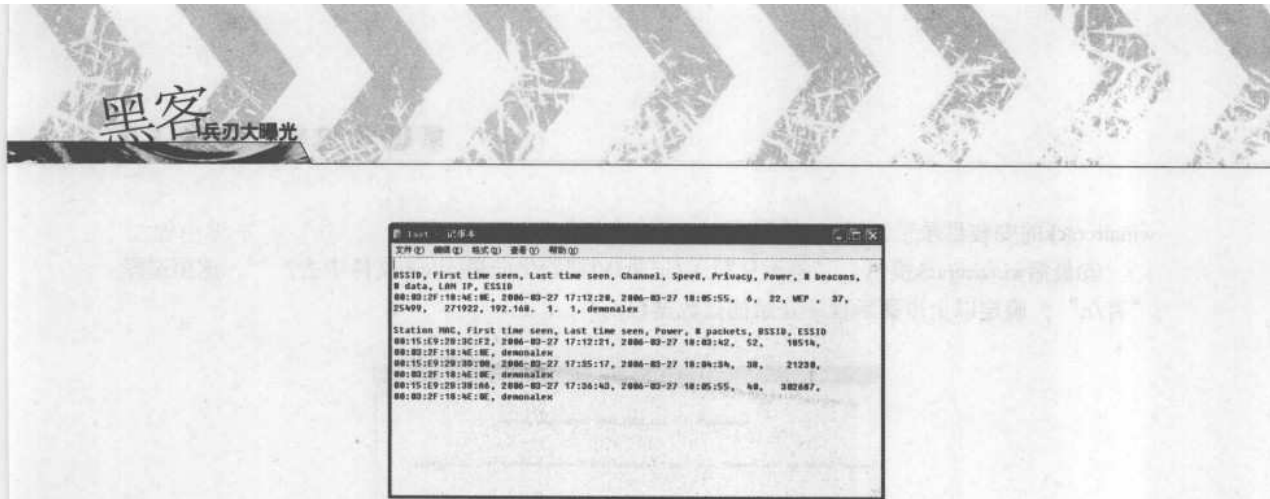
(2) 执行完一段时间后，会弹出“BSSID”的信息采集对话框，当“Packets”列的总数为300000时即可满足要求，如图10-55所示。根据经验所得：当该AP的通信数据流量极度频繁、数据流量极大时，“Packets”所对应的数值增长的加速度越大。当程序运行至满足“Packets”=300000的要求时按“Ctrl+C”结束该进程。



【图10-55】“BSSID”的信息采集对话框

(3) 找到winaircrack的安装目录，软件会生成last.cap与last.txt两个文件。其中last.cap为通用嗅探器数据包记录文件类型，可以使用ethereal程序打开查看相关信息；last.txt为此次嗅探任务最终的统计数据。使用“记事本/notepad”打开last.txt，如图10-56所示。

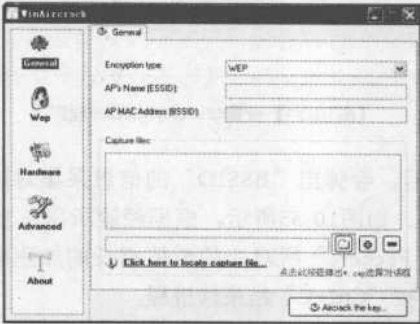
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



【图10-56】打开last.txt

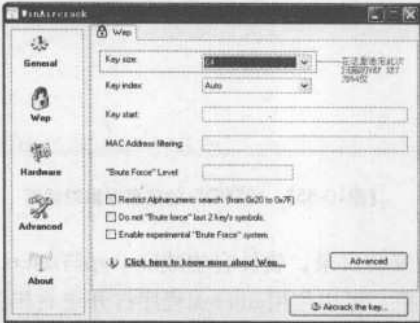
2.破解last.cap

(1) 首先执行WinAirCrack.exe文件，打开“WinAirCrack”主界面，如图10-57所示。单击红色框框部分的“文件夹”按钮，弹出“*.cap选定”对话框，选择last.cap文件，然后通过单击右方的“Wep”按钮切换主界面至“WEP破解”选项界面。



【图10-57】打开“WinAirCrack”主界面

(2) 选择“Key size”为64（目前大多数用户都是使用这个长度的WEP KEY，因此这一步骤完全是靠猜测定该值），最后单击主界面右下方的“Aircrack the key...”按钮，如图10-58所示。



【图10-58】“Kep”的选项界面

